AD-A284 502

(1)

3 June 94 Master's Thesis 2 Aug 93-3 Jun 94

Winning the Information War: Challenges of Providing Interoperable Information System Support to an Army-led Joint Task Force

MAJ James P. Kohlmann, USA

U.S. Army Command and General Staff College
Attn: ATZL-SWD-GD
Ft. Leavenworth, KS 66027-6900

Approved for public release; distribution is unlimited.

DTIC
ELECTE
SEP 16 1994
S B D

Joint interoperability is the key to enhancing the Army's warfighting capabilities in the years to come. The ability to provide fully interoperable information system support to an Army-led Joint Task Force (JTF) deployed halfway around the world is critical to the effectiveness of the JTF. This thesis examines the ability of an Army-led JTF to achieve interoperable information exchange today, and whether or not today's information systems will support the joint command, control, communications, computers and intellegence (C4I) concept for the future--"C4I for the Warrior" (C4IFTW). Information system interoperability is examined in the areas of command and control (C2), Air Task Order (ATO) exchange, and Secondary Imagery Dissemination (SID). Information system hardware, software, and program structures are investigated to determine which systems are best suited to be the basis for future interoperability standards. There is much work to be done by the Army to meet the C4IFTW requirements. Joint interoperabilty will not be effectively achieved if the Army continues on its present information system development course. In order to improve the joint interoperability of information systems, the Army must change its software development strategy to take advantage of software products developed by other services.

Joint Task Force, Interoperability, C4I for the Warrior, Force Projection, Information Systems C2, ATO, SID

119

UNCLASSIFIED UNCLASSIFIED UNCLASSIFIED

WINNING THE INFORMATION WAR: CHALLENGES OF PROVIDING INTEROPERABLE INFORMATION SYSTEM SUPPORT TO AN ARMY-LED JOINT TASK FORCE

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE

by

JAMES P. KOHLMANN, MAJ, USA
B.A., Marquette University, Milwaukee, Wisconsin, 1980

Fort Leavenworth, Kansas
1994

Approved for public release; distribution is unlimited.

94-30020

94 9 16 009

WINNING THE INFORMATION WAR: CHALLENGES OF PROVIDING INTEROPERABLE INFORMATION SYSTEM SUPPORT TO AN ARMY-LED JOINT TASK FORCE

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

JAMES P. KOHLMANN, MAJ, USA
B.A., Marquette University, Milwaukee, Wisconsin, 1980

Fort Leavenworth, Kansas
1994

Approved for public release; distribution is unlimited.

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ James P. Kohlmann

Thesis Title: Winning the Information War: Challenges of Providing Interoperable Information System Support to an Army-Led Joint Task Force

Approved by:

_____________________, Thesis Committee Chairman
LTC Herbert F. Merrick Jr., M.A.

_____________________, Member
CH (MAJ) Edward K. Maney, MDIV, Th.M.

_____________________, Member, Consulting Faculty
COL Kenneth R. Garren, Ph.D.

Accepted this 3rd day of June 1994 by:

_____________________, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

Dist
A-1

ABSTRACT

WINNING THE INFORMATION WAR: CHALLENGES OF PROVIDING INTEROPERABLE INFORMATION SYSTEM SUPPORT TO AN ARMY-LED JOINT TASK FORCE by MAJ James P. Kohlmann, USA, 120 pages.

Joint interoperability is the key to enhancing the Army's warfighting capabilities in the years to come. The ability to provide fully interoperable information system support to an Army-led Joint Task Force (JTF) deployed halfway around the world is critical to the effectiveness of the JTF. This thesis examines the ability of an Army-led JTF to achieve interoperable information exchange today, and whether or not today's information systems will support the joint command, control, communications, computers and intellegence (C4I) concept for the future--"C4I for the Warrior" (C4IFTW).

Information system interoperability is examined in the areas of command and control (C2), Air Task Order (ATO) exchange, and Secondary Imagery Dissemination (SID). Information system hardware, software, and program structures are investigated to determine which systems are best suited to be the basis for future interoperability standards. There is much work to be done by the Army to meet the C4IFTW requirements.

Joint interoperabilty will not be effectively achieved if the Army continues on its present information system development course. In order to improve the joint interoperability of information systems, the Army must change its software development strategy to take advantage of software products developed by other services.

ACKNOWLEDGEMENTS

My journey into the world of information system interoperability began in June 1989, when MAJ Bob Reynolds sent me to attend the Maneuver Control System version 11 Preliminary Design Review. Since that time, there have been countless soldiers, sailors, airmen, and marines who have contributed to my understanding of interoperability issues, and I thank them all.

I owe many thanks to COL Tom Nicholson, Director of the Battle Command Battle Lab (Ft. Gordon), who let me run interoperability demonstrations with an eye towards answering the "What if?" and "Why not?" questions rather than sticking to the way "things are supposed to be." He helped me to understand that the functional information requirements are the important things when supporting a Joint Task Force, not what service is in charge.

My committee members, LTC Herb Merrick, Jr., COL Kenneth Garren, and MAJ Ed Maney, have kept me focused and did not let me wander off on tangents. CPT Hunter Matthews helped me illustrate some key conclusions.

I want to thank my wife Cathie for tolerating the large chunks of time I spent on this thesis. Her counsel, proofreading, and editing skills made everything easier.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ACRONYM	MEANING
4GL	4th Generation Language
A2C2	Army Airspace Command and Control
AAR	After Action Reports
ACC	Air Combat Command
ACCS	Army Command and Control System
ACO	Air Coordination Order
ADA	Air Defense Artillery
ADS	Airspace Deconfliction System
AFATDS	Advanced Field Artillery Tactical Data System
AFFOR	Air Force component
AG	Adjutant General
AOC	Air Operations Center
API	Application Programming Interfaces
APS	ATO Planning System
ARFOR	Army Forces
ASAS	All Source Analysis System
ASCII	American Standard Codes for Information Interchange
ASD C3I	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASPO	Army Space Program Office
ATACC	Advanced Tactical Air Control Center
ATACCS	Advanced Tactical Air Command and Control System
ATCCS	Army Tactical Command and Control System
ATO	Air Tasking Order
AUTODIN	Automated Digital Network
AWIS	Army WWMCCS Information System
BCE	Battlefield Coordination Element
BFE	Blacker Front End
BOM	Bit-Oriented Message
C2	Command and Control
C4I	Command, Control, Communications, Computers and Intelligence
C4IFTW	C4I for the Warrior
CAC	Combined Arms Center
CAFMS	Computer Assisted Force Management System
CALL	Center for Army Lessons Learned
CASS	Common ATCCS Support Software
CCIR	Commander's Critical Information Requirements
CD-ROM	Compact Disk-Read Only Memory

CENTCOM	Central Command
CHS	Common Hardware Software
CINC	Commander-in-Chief
CINC-USAREUR	CINC-US Army Europe
CMD	Command
CN/CMS	Counter Narcotics/Command Management System
CNR	Combat Net Radio
COCOM	Combatant Command
COE	Common Operating Environment
COMAFFOR	AFOR component commander
COMARFOR	ARFOR component commander
COMM	Communications
COMSEC	Communications Security
CONUS	Continental United States
CoS	Chief of Staff
COTS	Commercial-Off-The-Shelf
CP	Command Post
CSS	Combat Service Support
CSSCS	Combat Service Support Command System
CTAPS	Contingency Theater Air Control (TACS) Automated Planning System
CVBG	Carrier Battle Group
DA	Department of the Army
DBMS	Database Management System
DCINC	Deputy CINC
DCS	Defense Communications System
DCS ENG	Deputy Chief of Staff for Engineering
DCS HNA	Deputy Chief of Staff for Host Nation Agreements
DCS IM	Deputy Chief of Staff for Information Management
DCS INT	Deputy Chief of Staff for Intelligence
DCS LOG	Deputy Chief of Staff for Logistics
DCS OPS	Deputy Chief of Staff for Operations
DCS PER	Deputy Chief of Staff for Personnel
DCT	Digital Communication Terminal
DDN	Defense Data Network
DDS	Data Display Services
DET	Data Entry Terminals
DISA	Defense Information Systems Agency
DISC4	Directorate for Information Systems, Command, Control, Communications and Computers
DMA	Defense Mapping Agency
DMS	Defense Messaging System
DoD	Department of Defense
DPS	Data Processing System
DSD	Deputy Secretary of Defense
DSNET	Defense Secure Network
E-MAIL	Electronic Mail
EAC	Echelons Above Corps
ECB	Echelons Corps and Below
EO	Engagement Operations

EOTDA	Engagement Operations Tactical Data Analysis
EW	Electronic Warfare
FAADC3I	Forward Area Air Defense C3I system
FAST	Forward Area SIDS and TRE
FEC	Forward Error Correction
FISH	Forces Command (FORSCOM) Imagery Server Host
FIST	Fleet Imagery Support Terminal
FLC	Force Level Control
FSS	FORSCOM SID System
FTP	File Transfer Protocol
FY	Fiscal Year
GCCS	Global Command and Control System
GSORTS	Global Status of Resources and Training
GUI	Graphic User Interface
HDD	Hard Disk Drive
HF	High Frequency
HOL	Higher Order Language
HP	Hewlett Packard Corporation
HP-UX	HP version of the UNIX operating system
HQ CMDT	Headquarters Commandant
H/W	Hardware
IAS	Intelligence Analysis System
IBP	Integrated Business Package
IG	Inspector General
IEW	Intelligence and Electronic Warfare
IMOM	Improved Many-on-Many
INTEL	Intelligence
ISC	Intersoftware Communications
J6I	JCS J6 integration office
JA	Judge Advocate
JCS J-6	JCS Directorate for Command, Control, Communications and Computer systems
JCS	Joint Chiefs of Staff
JCSE	Joint Communications Support Element
JDISS	Joint Deployable Intelligence Support System
JDS	Joint Deployment System
JFACC	Joint Forces Air Component Commander
JIC	Joint Intelligence Center
JIEO	Joint Interoperability and Engineering Organization
JITC	Joint Interoperability Test Center
JMEM	Joint Munitions Effectiveness Manual
JMCIS	Joint Maritime Command Information System
JOPES	Joint Operation Planning and Execution System
JOTS	Joint Over the Horizon Targeting System
JSOTF	Joint Special Operations Task Force
JTF	Joint Task Force
JUDI	Joint Universal Data Interpreter
LAN	Local Area Network
LCU	Lightweight Computer Unit
LNO	Liaison Officers
LOG	Logistics

MAGTF	Marine Amphibious Group Task Force
MAGTF Log/AIS	MAGTF Logistics Automated Information Systems
MARFOR	Marine Forces
MCEB	Military Communications Electronics Board
MC	Major Commands
MCS	Maneuver Control System
MEB	Marine Expeditionary Brigade
MFATDS	Multiservice Field Artillery Tactical Data System
MIL-SPEC	Military Specifications
MIL-STD	Military Standard
MILNET	Military Network (Unclassified)
MLS	Multi-Level Security
MO	Magneto-optical
MP	Military Police
MS-DOS	Microsoft Disk Operating System
MSC	Major Subordinate Commands
MSE	Mobile Subscriber Equipment
MTA	Message Transfer Agent
MTCCS	Marine Tactical Command and Control System
NATO	North Atlantic Treaty Organization
NAVFOR	Naval Force
NBC	Nuclear, Chemical and Biological
NCA	National Command Authority
NIC	Naval Intelligence Center
NIC	National Intelligence Centers
NICP	National Inventory Control Point
NITF	National Imagery Transmission Format
NTCS-A	Naval Tactical Command System Afloat
NTDS	Naval Tactical Data System
OB	Order of Battle
ODS	Operation Desert Storm
OS	Operating System
OSS	Operational Support System
OTAU	Over the Air Updating
PC	Personal Computer
PED	Packet Encryption Device
PEO	Program Executive Office
PEO-CCS	PEO for Command and Control Systems
PEO-COMM	PEO for communications
PEO-IEW	PEO for Intelligence and Electronic Warfare
PLRS	Position Location Reporting System
PM	Provost Marshal
PM	Program and/or Product Managers
PNMC	Packet Network Management Center
POSIX	Portable Operating System Interface
QUID	Quadrilateral Interface Device
R&D	Research and Development
RAAP	Rapid Application of Air Power
RAM	Random Access Memory
REM	Route Evaluation Module
RDBMS	Relational Database Management System

RISC	Reduced Instruction Set Computer
ROE	Rules of Engagement
RPC	Remote Procedure Call
SCC	System Control Center
SCO UNIX	Southern Califoria Operating System version of UNIX
SDNS	Secure Data Network System
SICPS	Standard Integrated Command Post Shelter
SID	Secondary Imagery Dissemination
SQL	Structured Query Language
SRI	Standing Request for Information
STACCS	Standard Theater Army Command and Control System
STAMIS	Standard Army Management Information System
STDN	Secure Tactical Data Network Demonstration
STU-III	Secure Telephone (version 3)
SURG	Surgeon
SWO	Staff Weather Officer
S/W	Software
TAC CP	Tactical Command Post
TACCIMS	Theater Automated Command and Control Information Management System
TASDAC	Tactical Secure Data Communications system
TCC	TeleCommunication Centers
TCDN	Tactical Communication Distribution Node
TCP/IP	Transmission Control Protocol/Internet Protocol
TDS	Tactical Data Systems
TISD	Tactical Integrated Situation Display
TNS	Tactical Name Server
TOD	Time of Day
TPN	Tactical Packet Network
TRADOC	Training and Doctrine Command
TRE	Tactical Receive Equipment
TRI-TAC	Tri-service Tactical Communications
TSM	TRADOC System Managers
TSM-ABCS	TSM for Army Battle Command Systems
UB2	Unified Build version 2.0
USA CECOM	US Army Communications and Electronics Command
USMTF	US Message Text Format
USTRANSCOM	United States Transportation Command
VADM	Vice Admiral
VHF	Very High Frequency
WAN	Wide-Area Network
WIN	WWMCCS Information Network
WISDN	Wireless Integrated Services Digital Network
W/S	Workstation
WWMCCS	World Wide Military Command and Control System

CHAPTER 1

INTRODUCTION

The Problem

The US Army has recognized that it cannot fight alone.[1] Senior leaders also recognize that the Army will fight or deploy combat forces in a range of strategic environments--war, conflict and peacetime.[2] Joint, Combined and Interagency operations are now key parts of our new doctrine as stated in FM 100-5, Operations. Unfortunately, it is easier to say that US forces will fight in a joint environment than it is to do so.

The change in US strategy--regional orientation, uncertain and unknown threat, smaller Total Force, theater Commander-in-Chiefs (CINCs)--not service chiefs driving the planning process,[3] creates new requirements and challenges in command and control. The old way of doing business is over. The commander of a Joint Task Force (JTF) halfway around the world, must instantly communicate with the commanders of the forces assigned to the JTF and the theater Unified or Specified CINC. Access to the National Command Authority (NCA) may also be required (Figure 1.).

The purpose of this communication is to exchange information vital to the success of the JTF commander's

mission. Usually, the JTF headquarters receives intelligence and imagery from National Intelligence Centers (NICs) or Joint Intelligence Center (JIC) or other national sources. The JTF Commander must be ready to receive changes to directives or Rules of Engagement (ROE) directly from the CINC or the National Command Authority (NCA). The JTF commander must disseminate this information quickly

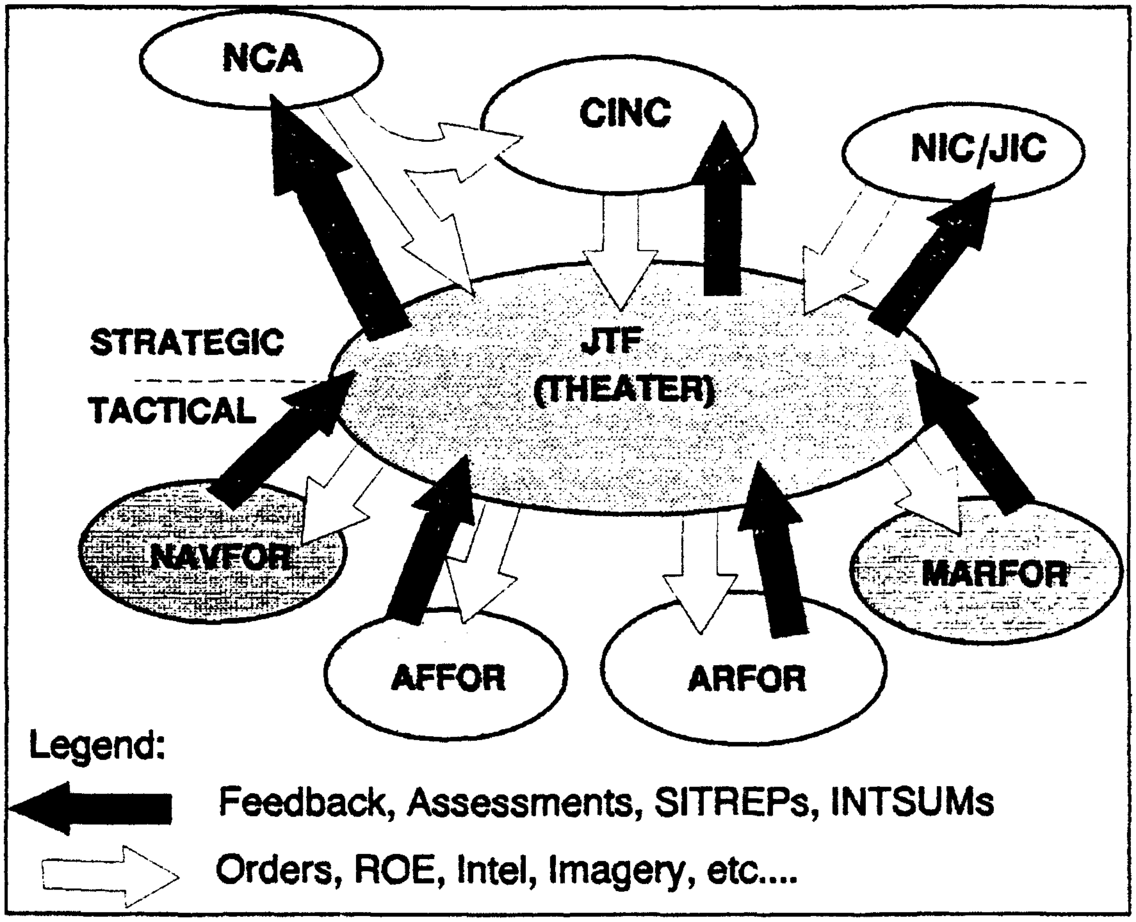

Figure 1. Information Flow to a JTF

throughout the theater to whoever needs it, regardless of service. Likewise, information must be sent back to the CINC or the NCA in a timely manner.

Current CINC and service-unique command and control (C2), communications, computer and intelligence (C4I) systems do not support an integrated approach to providing required information to the warfighter. Direct information sharing between the services and allies at the JTF level presents significant challenges. The key challenge for the JTF commander is to receive information from each service information system, correlate the data and put it into usable form, disseminate the information and the related decision, and act on it faster than the enemy can act. This problem will face all forces working in a joint environment.

Three fundamental issues have emerged in the area of joint interoperability from the lessons learned in Operations Urgent Fury, Just Cause and Desert Shield/Desert Storm. These issues are so significant that the Joint Chiefs of Staff (JCS) J-6 (Command, Control, Communications and Computers Directorate) directed that they be examined during the third Secure Tactical Data Network Demonstration (STDN-3) held at Fort Gordon, Georgia, from 16 November through 11 December 1992. The areas explored during STDN-3 are exchange of Command and Control (C2) information,[4] distribution of airspace coordination/control measure and

the Air Tasking Order (ATO),[5] and Secondary Imagery Dissemination (SID) at the tactical level.

Background

As a forward-deployed force, the Army in Europe was self-sustaining and had minimal information exchange requirements outside the existing theater/tactical Army units. A mature theater of operations had been established, and the doctrinally-prescribed communications interfaces to the North Atlantic Treaty Organization (NATO) allied forces and to the Air Force headquarters in theater also established. The US Navy, Marine Corps, and Special Forces assets were largely ignored. Information exchange within the Army and with other services or allies was accomplished through the use of the formal record traffic system--the AUTOmated DIgital Network (AUTODIN), or by Liaison Officers (LNOs), voice telephone or radio communication, or by facsimile.

Throughout the 1980s, each branch of service undertook major weapons systems modernization programs. The services put a significant amount of effort into developing more sophisticated intelligence gathering equipment, "smart" weapons, and automated control systems for the weapons. These modernization initiatives created "stovepipe" technical information systems that met the needs of the weapons system within the individual service. Although there are some notable efforts at interservice cooperation

(some data protocol standardization between the Navy and Air Force), the services put little effort into joint interoperability requirements for information systems during the acquisition process.

These parallel information system developments resulted in islands of information at the end of the stand alone, or stovepipe systems, within the services that comprise the JTF. The Department of Defense (DoD) faces many obstacles in breaking the information out from these "islands" and putting it directly in the hands of those who need it most, regardless of service affiliation. In short, deployed combat forces are constrained to some extent by service-unique C2 or C4I systems. Advances in automation and communications have brought us to the brink of the third major revolution in the area of command and control. The first breakthrough was the tactical use of the telegraph during the American Civil War. The second was the extensive use of the wireless radio by mechanized and armored forces during World War II. The third is the integration of automated decision support aids into tactical command posts.

In 1991, Vice Admiral (VADM) Richard C. Macke, then the Director of the J-6 for the Joint Chiefs of Staff (JCS), established a concept that he called "C4I for the Warrior." This idea called for increased interoperability between service communication systems and information systems. Implementing this concept requires increased

interoperability between service communication systems and information systems. These systems will allow the warfighter to "plug in" where ever he is on the battlefield and "pull" the required data from where ever it is located. VADM Macke became the prime joint advocate for what, since 1989, the Army had been calling the "seamless architecture." With the weight of the JCS J-6 behind it, "C4I for the Warrior" (C4IFTW) became an accepted objective of all the services.[6] Over the past two years, each of the services has outlined their strategies to implement C4IFTW.

All services have moved toward automating tactical and operational mission-related functions and are taking advantage of new technology in the information transfer area. Current efforts include developing more and better tactical information systems and using Electronic Mail (E-Mail) under field conditions. Services are in the process of moving message traffic from AUTODIN to its replacement--the packet-based Defense Messaging System (DMS).

The importance of interoperability is highlighted by recent congressional directives to the Assistant Secretary of Defense for Command Control Communications and Intelligence (ASD C3I) to ensure that tactical forces have access to Defense Data Network (DDN) data network gateways. Other directives from the Deputy Secretary of Defense (DSD)[7] and ASD C3I[8] recognize the need for common information systems and that there will be some loss of operational

capabilities during the transition to standard, DoD-wide information and command systems. The National Military Strategy requires that a continental United States (CONUS)-based force be capable of projecting corps and division-sized elements in contingency missions. Seamless communications systems and exchange of information between tactical and strategic information systems are required in order for those projected forces to operate effectively.

Research Question

This thesis identifies and explores the challenges that face the commander of an Army-led Joint Task Force (JTF) when putting together a coherent C4I information system architecture for the forces on the ground. The research question is as follows: Can current C4I information systems link key operational forces in an Army-led Joint Task Force (JTF)? This thesis examines the capabilities of some representative Army, Navy, Marine and Air Force automated information systems and assess their capabilities in C2 information exchange, ATO distribution, and tactical secondary imagery dissemination (SID). Supporting questions answered include the following:

How well do service information systems meet the objective requirements for joint interoperability established by the C4I for the Warrior[9] concept?

What levels of computer hardware and information system software interoperability currently exist?

Assumptions

The force structure and the supporting C4I equipment are keys to understanding the scope and complexity of the problem. In identifying the makeup of the JTF, the assumption is that all service components will bring and employ fielded C4I systems in a doctrinally-correct manner.

A typical Army-led JTF may be based on the following structure: a mechanized US Army Corps, with two subordinate divisions (1 Armor, 1 Mechanized). The corps commander is the JTF commander (COM JTF), with the deputy corps commander serving as the Army Forces (ARFOR) component commander (COM ARFOR). If the JTF is deployed in the Central Command (CENTCOM) Area of Responsibility, then The Commander-in-Chief of US Central Command (CINC CENTCOM) exercises Combatant Command (COCOM) over the JTF. Third (US) Army provides C4I augmentation to the corps staff.

The Naval Force (NAVFOR) consists of a Carrier Battle Group (CVBG). Marine Forces (MARFOR) are a Marine Expeditionary Brigade (MEB) already deployed from an Amphibious Task Group. The Air Force (AFFOR) component is a composite wing. The AFOR commander (COM AFFOR) serves as the Joint Forces Air Component Commander (JFACC). A Joint Special Operations Task Force (JSOTF) is also part or the JTF. The Joint Communications Support Element (JCSE) has not been deployed to support the JTF Headquarters.

Each service has developed dedicated data networks to support its tactical information systems. Each service's data network must interoperate with strategic data networks. Strategic data distribution is segregated according to classification level by the various components of the Defense Data Network (DDN). It consists of the unclassified Military Network (MILNET) and the Defense Secure Network (DSNET), which is segregated by security classification: DSNET 1 (SECRET - S), DSNET 2 (TOP SECRET - TS), and DSNET 3 (TOP SECRET/SPECIAL COMPARTMENTED INFORMATION - TS/SCI).

Tactical distribution of data will be accomplished via a single Tactical Packet Network (TPN) within the Army--a combination of the Mobile Subscriber Equipment (MSE) and Tri-service Tactical Communications (TRI-TAC) packet networks. The US Marine Corps will use their newly developed Tactical Communication Distribution Node (TCDN). The Air Force will use their Tactical Secure Data Communications (TASDAC) system to distribute internal Air Force information. For more information on communications equipment, see Appendix B.

Limitations

There is little written on the interoperability of automated information systems which support the JTF and why it is important to have joint exchange of information. Much of the input in this area comes from test reports and interoperability demonstrations, which reflect only

technical analysis and not operational analysis of user requirements. Time and the availability of data from system program offices are limiting factors.

Delimitations

To give the research focus, three key areas will be addressed: exchange of command and control information (C2), exchange of the Air Task Order (ATO), and exchange of tactical imagery. These three areas were chosen because of the importance placed on these areas in Desert Shield/Desert Storm After Action Reports (AARs).

There are many issues relevant to linking C4I systems in an Army-led JTF. Since each service maintains its own communication systems to support C4I, there are many interoperability issues in this area that effect interoperability of information systems. The communications systems that support each service's information systems will only be defined, and communication system issues will only be presented when they impose significant limitations on the transfer of information between components of the JTF.

JSOTF communications or information systems will not be discussed. While the communications systems used by the JSOTF are well defined, the information systems that support the JSOTF have highly classified aspects to them. To keep the paper narrow in focus and to avoid possible classification issues, the JSOTF will not be addressed.

Information Systems

Current Strategic Information Systems

The strategic and operational echelons of the Department of Defense (DoD) use several different planning and execution systems. These systems are tied together under the World Wide Military Command and Control System (WWMCCS) and the WWMCCS Information Network (WIN). The WWMCCS, which was significantly upgraded and fielded in 1978, is an information system which uses strategic DoD communications systems to link warfighting and supporting Commanders-in-Chief (CINCs), the services and the National Military Command Authority at critical command and control (C2) locations to each other. JTFs are also connected to WWMCCS when deployed. Different software programs are used depending on the function being performed.

For example, a component of the Joint Operation Planning and Execution System (JOPES), the Joint Deployment System (JDS), may be used to develop deployment plans or courses of action. WWMCCS is normally used to distribute the plans for comment to all concerned agencies, activities and CINCs.[10] Although WWMCCS provides useful information to the joint user, it is not easy to use and requires specially trained officers and enlisted personnel to operate the system and retrieve data. Although there have been many efforts to update and modernize WWMCCS, the Deputy Secretary of Defense (DSD) decided that it should be replaced.[11]

Future Strategic Information Systems

The Global Command and Control System (GCCS) has been designated as the replacement for WWMCCS in order to implement the C4I For The Warrior concept at the strategic level. To add functionality, increase system performance and reliability, GCCS

> will become the single, global command, control, and communications, and intelligence system to support the war fighter, whether from a fox hole or from a command post.[12]

According to the GCCS integration plan, WWMCCS will be replaced incrementally. Two of the first three packages to be developed and fielded under GCCS will be functional replacements for the Joint Operation Planning and Execution System (JOPES) and the Global Status of Resources and Training System (GSORTS). The third package will increase the functionality of GCCS beyond the capabilities of WWMCCS by adding capabilities from the Navy's Operational Support System (OSS)[13] and the Air Force's Contingency Theater Air Control (TACS) Automated Planning System (CTAPS). The GCCS common operating environment (COE) is based on software modularity, portability and scalability, as well as a standardized, open operating system and the use of standard data elements--all requirements of C4IFTW.

Army Information Systems

Echelons Above Corps (EAC)

The Army Command and Control System (ACCS) is a system of information systems. At Echelons Above Corps (EAC), the primary C2 system is the Standard Theater Army Command and Control System (STACCS). STACCS provides commanders and staff at EAC with data-driven situation displays, map data,and briefings. STACCS has a deployable network of computers and peripherals operating at the SECRET level in the system-high security processing mode.

STACCS primarily provides for the reporting, coordination and control of force reception and onward movement, redeployment, intelligence information , rear area operations, joint and combined operations, and host nation support operations.[14] It provides the following capabilities: Electronic Mail, Data Communications, Local and Shared Database Management, Situation Map Graphics, Word Processing, Report Generation, Applications and Decision Support Tools, and Network/System Management.

STACCS is a deployable theater-level Command and Control (C2) system that provides automation support to the Theater Army Headquarters, Major Subordinate Commands (MSC), subordinate commands, and liaison officers (LNOs) when required. The system provides secure exchange of information between headquarters staff and subordinate units during peace, transition to war, and war. Information

exchange with allied and coalition staff officers is accomplished by providing dedicated STACCS terminals to LNOs at major information nodes. These LNO positions will normally be established in the combined or JTF command post (CP). Figure 2 shows the functional relationships between the Theater Army HQ staff agencies and the external C2 environment.

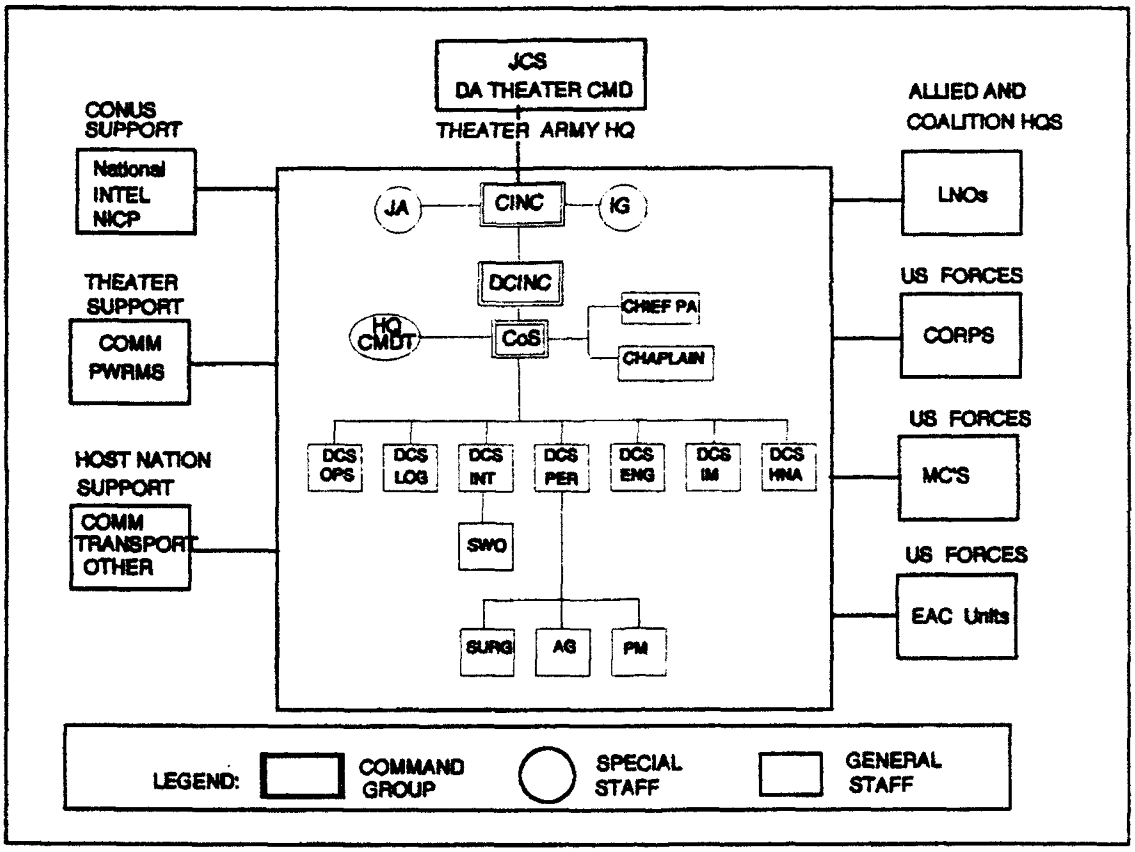

Figure 2. STACCS Functional Relationships

SOURCE: US Army Europe (USAREUR), UTACCS/STACCS Fact Sheet, (HQ, USAREUR, 1992).

STACCS potentially ties to the strategic level Army Worldwide Military Command and Control System (WWMCCS) Information System (AWIS) and the tactical-level Army Tactical Command and Control System (ATCCS). Components of the Army Tactical Command and Control System (ATCCS) will eventually be able to exchange information with STACCS.

STACCS, although in the process of developing an architecture which does not require dedicated tactical and strategic communications systems, currently consists of a network of information nodes configured individually with processors and peripheral support devices. The workstations at the primary nodes share access to communications and peripheral devices and also transmit intra-node data over a high speed local area network (LAN). Each node has a gateway and communications security (COMSEC) equipment that provides secure communications with other nodes via a dedicated strategic packet-switched network. Remote terminals can dial-up into the nodes via commercial lines and communications concentrators with appropriate COMSEC equipment. Figure 3 shows the topology of the dedicated STACCS network.

Echelons Corps and Below (ECB)

At ECB, the ATCCS consists of the Maneuver Control System (MCS), the All Source Analysis System (ASAS), the Advanced Field Artillery Tactical Data System (AFATDS), the Forward Area Air Defense C3I system (FAADC3I), and the

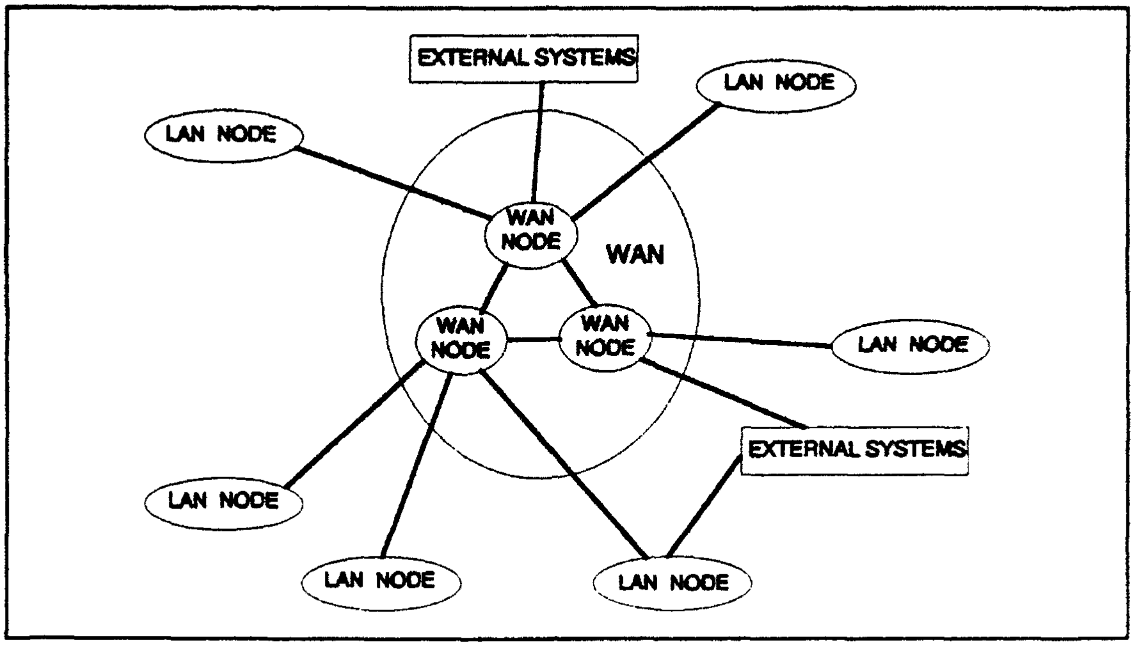

Figure 3. STACCS Network Topology

SOURCE: PM OPTADS, STACCS System Specification Ver. 1.1, (HQ, USACECOM, 1993).

Combat Service Support Command System (CSSCS). The ATCCS provides automated tools to assist the commander and staff in synchronizing the efforts of the combined arms team. Through proper information management, the ATCCS reduces the time to develop and distribute operational plans, orders, overlays, intelligence and logistics information.[15]

These systems have been in research and development for the last five to ten years and are in the process of being fielded. MCS, which has been fielded to all armored or mechanized corps and divisions in the Army, is the most widely used system. Both the ACCS and the ATCCS information

systems have established requirements to exchange data with each other and with strategic information systems external to the TPN. Other systems, including the Standard Army Management Information System (STAMIS), Counter Narcotics/Command Management System (CN/CMS), and intelligence systems will also require strategic access from the TPN.

MCS is a Corps-wide system designed to provide automated assistance to the commander and his staff, and to facilitate the management of information and the execution of the commander's concept of operation. The system is supposed to improve the commander's ability to swiftly collect, coordinate, and act on near real time battlefield information. Finally, the MCS system is intended to support information exchanges between the battlefield functional areas: Maneuver Control, Air Defense Artillery, Fire Support, Intelligence/Electronic Warfare, and Combat Service Support. This capability places MCS as the "backbone" of the overall Army Tactical Command and Control System (ATCCS).

MCS uses all standard Army tactical communications, and it employs the Army standard character-oriented message text formats to support NATO and Joint Service Interoperability. Databases are maintained at each echelon, with redundancy at each echelon. Specified data or displays can be directed to any device in the entire network on an

as-needed basis. Terrain maps are provided as an integral capability, with the information overlaid in graphic form about both friendly and enemy units.[16] The MCS operational concept is shown in Figure 4.

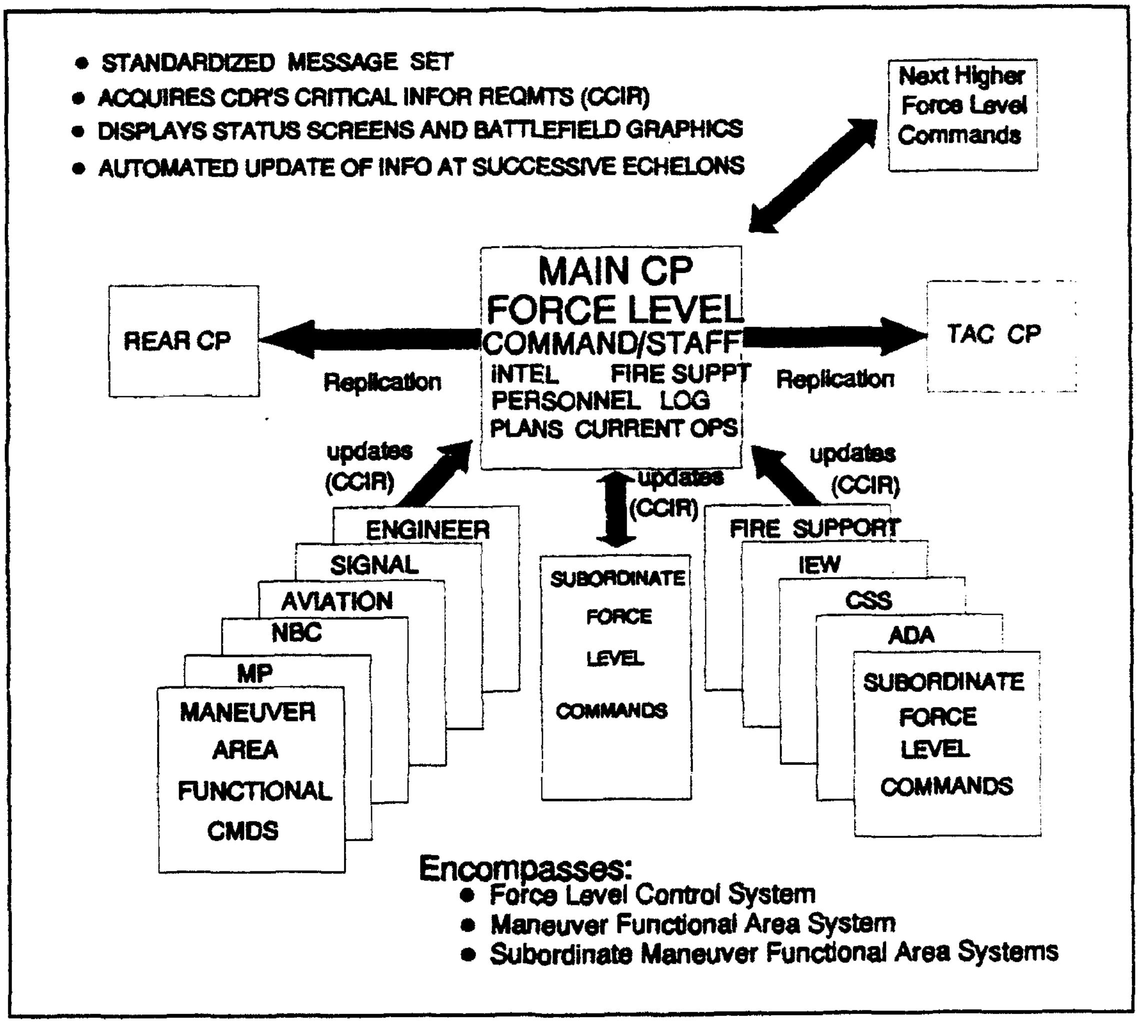

Figure 4. MCS Operational Concept

SOURCE: Briefing, US Army TRADOC System Manager for MCS, MCS Program Briefing, (HQ, TRADOC, October 1991).

Messages and reports can also be displayed using the Integrated Business Package (IBP). IBP can extract selected information from the MCS data bases, and it can manipulate the data using the word processing or spreadsheet applications within the program. Files created in IBP can be saved, recalled, edited and/or transmitted between devices in the network. The IBP provides templates for generating recurring reports or messages that are not pre-formatted in the MCS operational program. Other MS-DOS applications, such as Multimate, Lotus 1-2-3, and Harvard Graphics may be used on MCS hardware to prepare documents as needed.[17]

Marine Corps Information Systems

Marine Corps Tactical Data Systems (TDSs) exchange real-time or near real-time data. They communicate primarily to update databases automatically and without human intervention. Examples include passing Time of Day (TOD), position location information. Examples of Marine Corps TDSs are as follows: Marine Tactical Command and Control System (MTCCS), Multiservice Field Artillery Tactical Data System (MFATDS), Position Location Reporting System (PLRS), Digital Communication Terminal (DCT), Advanced Tactical Air Command and Control System (ATACCS), Intelligence Analysis System (IAS), and Marine Amphibious Group Task Force (MAGTF) Logistics Automated Information Systems (MAGTF Log/AIS). MTCCS, ATACCS, MFATDS, MAGTF

Log/AIS and IAS all have requirements to interface with strategic systems through the TCDN.

Air Force Information Systems

The Contingency Theater Air Control (TAC) Automated Planning System (CTAPS) is the capstone program for tactical battle management in the Air Force; it is similar to the Army's ACCS or ATCCS programs.

CTAPS Background

The Air Tasking Order (ATO), along with the Air Coordination Order (ACO), is the central document published by the Air Operations Center (AOC) for the direction of air operations and specific individual unit and mission operational tasking. This document can be small for a contingency, single-wing operation, or a large 2000-3000 sortie document, for theater operations such as Desert Storm. The method of passing the ATO to joint participants by formal record traffic or air courier during Operation Desert Storm was determined to be unacceptable in the future. As a result, an effort was initiated to integrate CTAPS with the Navy Joint-Over-the-Horizon Targeting System (JOTS) for ATO passing and mission status reporting. Work is ongoing with the Army Maneuver Control System and STACCS, and the Marine ATACCS to achieve the same results.[18]

CTAPS Description

CTAPS has software modules for performing tasks critical to conduct of the air war: intelligence gathering and distribution, targeteering, weaponeering, route evaluation, Electronic Warfare (EW) analysis, situations display, and Air Task Order (ATO) planning and management. CTAPS software modules are shown in Figure 5.

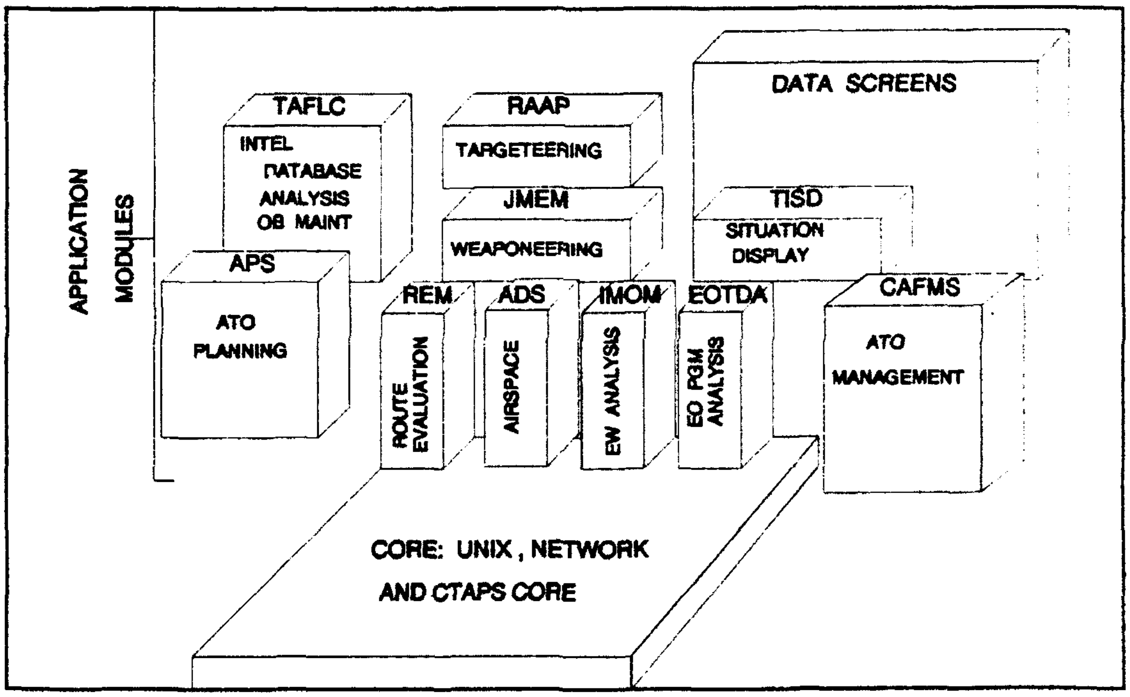

Figure 5. CTAPS Software Architecture

SOURCE: US Air Force Air Combat Command (ACC), CTAPS Program Summary, (USAF ACC, June, 1992).

While most of these functions are Air Force unique, the ATO requires extensive coordination within a theater of operations. CTAPS needs to exchange information with the

Army's STACCS, the Marines' ATACCS, and the Navy's Operational Support System (OSS). In December 1991, CTAPS was designated as the standard for ATO software and protocols. The CTAPS program is developing interfaces with other Air Force and service unique systems, including the Air Mobility Command C2 Information Planning System, the Army Maneuver Control System (MCS), the US Naval Tactical Command System Afloat (NTCS-A) system, and the US Marine Corps Advanced Tactical Air Control Center (ATACC) system.

Navy Information Systems

The Navy's Joint Maritime Command Information System (JMCIS) integrates information systems that were considered separate programs until 1993. These systems include the Naval Tactical Command System-Afloat (NTCS-A), the strategic Operational Support System (OSS), and the Joint-Over-the-Horizon Targeting System (JOTS). These systems, which use Unified Build version 2.0 (UB2) software as the basis for their interoperability, are now under one configuration manager. All systems run on a UNIX-based hardware platform. JMCIS automates the C2 process and supports multiple communications interfaces and links to shipboard or land-based systems. It processes strategic or tactical information received from a variety of sources and automatically correlates this data with the existing tactical databases from the Naval Tactical Data System (NTDS) which are fed by data links from ships or aircraft.

The tactical database is then used to generate computer graphic images at any workstation and provide timely information to the commander.[19]

The NTCS-A, the cornerstone of the Navy's afloat C4I system, is capable of providing the same information to shore stations running OSS software. It provides the shipboard user with timely data from multiple sources, including aircraft and intelligence services. NTCS-A is the focus of many integration efforts. The Navy has already integrated a CTAPS module into NTCS-A for ATO generation and distribution, and is in the process of adding modules that are Marine Corps-specific (USMC Position Location Reporting System (PLRS)) and joint-specific.

Imagery Software

Secondary Imagery Distribution (SID) has emerged as a critical need for battlefield commanders. Many government agencies, including the Army Space Program Office (ASPO) and the Naval Intelligence Center (NIC) have cooperated to develop standards for the transmission of imagery. The implementation of National Imagery Transmission Format (NITF) and standard imagery protocols have allowed the dissemination of imagery across service lines with no problems. The key to this success story is the certification process that has been established. The Joint Interoperability and Engineering Organization (JIEO) tests and certifies all software packages that are designed to

display imagery. This process ensures that all fielded software is interoperable and that SID information can be easily disseminated.

ASPO has developed and certified a software package called the FORSCOM SID System (FSS). This software package can be installed on any Personal Computer (PC) and can display images which are NITF compliant. This capability will give any commander in the field the ability to see pictures of the battlefield in a timely manner. Imagery can be exchanged with Army ASPO equipment or with the Navy's Fleet Imagery Support Terminal (FIST).

Defense Messaging System (DMS)

The Department of Defense (DoD) is moving rapidly toward implementation of the Defense Messaging System (DMS). The objectives of DMS are reduction of cost and staffing while maintaining the current levels of message service and security. This system will replace AUTODIN with an automated writer-to-reader packet-based message-handling system and will be the basis for future messaging within the entire DoD. It will be implemented in three phases. The first, which is underway, is characterized by integration of AUTODIN and DDN, the automation of TeleCommunication Centers (TCCs) and the extension of message delivery to the office Personal Computer (PC).

The second phase, which begins in 1996, calls for the elimination of all AUTODIN switching centers and the

incorporation of a Multi Level Secure (MLS) Secure Data Network System (SDNS). The implementation of DMS will have significant impacts on all user-owned and operated information systems after 1996. If tactical users do not support the evolution to DMS, there will be incompatibility between the tactical and strategic information systems. This incompatibility will restrict each element and service's ability to send and receive information across echelons.

Significance of the Study

Much progress has been made in the area of information system interoperability. While systems are not fully interoperable today, this study validates the planned interoperability improvements to existing systems, and points out problems with the Army's approach to solving these problems where appropriate. In the future, interoperable C4I systems will be capable of fully supporting Army-led JTFs. However, the Army must act soon to improve the interoperability of its information systems.

The Army is involved in an extensive effort to digitize the battlefield. Digitizing the battlefield offers a way to take advantage of emerging technology to improve the Army's warfighting capabilities. Because the Army's digitization of the battlefield touches virtually every weapons system, command and control (C2), intelligence and logistics system, the Army's initiatives must be tied to

joint efforts to standardize command, control, communications, computers and intelligence (C4I) systems. A fully digitized battlefield requires information and communications systems that are interoperable between the services at various command echelons.

Interoperability exists between most information systems at the most basic level--file transfer. How useful file transfer is in accomplishing the JTF mission is questionable. There appear to be problems in establishing and maintaining standards that support the user requirements of all services, and that no truly defined automation standards exist for a JTF. This thesis supports some of the key objectives as stated in the JCS C4I for the Warrior[20] concept. This study should enhance the Department of Defense's (DoD) understanding that there are problems facing the services which could cause a JTF to fail its mission through a failure in automation interoperability.

Endnotes

1. Department of the Army, FM 100-5, Operations, (Headquarters, Department of the Army, June 1993), 2-2.

2. FM 100-5, 2-0.

3. Chairman, Joint Chiefs of Staff, National Military Strategy of the United States, (US Government Printing Office, Washington D.C., Jan 1993), 26.

4. Department of Defense, Final Report to Congress: Conduct of the Persian Gulf War, (US Government Printing Office, Washington D.C., April 1992), 574-575.

5. Conduct of the Persian Gulf War, 552, 574.

6. Chairman, Joint Chiefs of Staff, C4I for the Warrior, (US Government Printing Office, Washington D.C., June 1992).

7. DSD Memorandum, Accelerated Implementation of Migration Systems, (DSD, Washington D.C., October 1993).

8. ASD C3I Memorandum, Selection of Migration Systems, (ASD C3I, Washington D.C., November 1993).

9. C4I for the Warrior, 9 - 12.

10. Chairman, Joint Chiefs of Staff, JCS Pub 5-00.2 Joint Task Force (JTF) Planning Guidance and Procedures, (US Government Printing Office, Washington D.C., Jun 1988), III-2.

11. DSD Memorandum, Accelerated Implementation of Migration Systems, (DSD, Washington D.C., October 1993).

12. Defense Information Systems Agency, GCCS Common Operating Environment, (Defense Information Systems Agency, Washington D.C., Dec 1993), ii.

13. Joint Interoperability and Engineering Organization, GCCS System Integration Plan, (Defense Information Systems Agency, Washington D.C., Dec 1993), 1.

14. Department of the Army, FM 24-7, Army Tactical Command and Control System (ATCCS) System Management Techniques (DRAFT), (Headquarters, Department of the Army, March 1993), 49-50.

15. FM 24-7, 3,4.

16. US Army Combined Arms Center (USA CAC), Organizational and Operational Plan (O&OP) for the Family of Maneuver Control System (MCS), (Ft. Leavenworth, KS, 1989), 10-25.

17. STDN-3 Report, I-17 - I-19.

18. STDN-3 Report, I-7 - I-11.

19. STDN-3 Report, I-21.

20. C4I for the Warrior, 15.

CHAPTER 2

LITERATURE REVIEW

Summary

There are many references on JTF operations and planning JTF operations. Technical publications from the joint staff detail the intricacies of installing, operating and maintaining communications in support of a JTF- or a CINC-level command. Reference and technical documents exist on the requirements for information system interoperability. Because the fielding of dedicated data networks and automated decision aids and information systems is in its infancy, little is written about the specific area of this investigation.

Joint Documents

The National Military Strategy of the United States (1992) establishes the framework for military operations that are consistent with the National Security Strategy. It calls for many fundamental changes in the way the services have prepared for conflicts. It places emphasis on the desirability of supporting coalition efforts as a way to counter regional instabilities. It also calls for joint operations to react to situations. It says that the joint

force will be tailored to the situation and will be drawn from all services, both forward-deployed and CONUS-based assets. The document cites recent examples of operations and emphasizes that adaptive, flexible planning, and control are paramount in the execution of our strategy.

Conduct of the Persian Gulf War is the official after action report to the US Congress by the Department of Defense (DoD). It provides information on how the Iraqi threat was countered by all services. The report is the result of interviews with senior participants, review of official documents, and other official sources, including the Office of the Secretarty of Defense (OSD) and the Joint Staff. The annexes to the report provide observations and conclusions into many areas of the Desert Storm campaign, including intelligence, command, control and communications interoperability issues.

C4I for the Warrior provides an overview of the requirements that must be met in order for the services to be truly interoperable and exchange information "seamlessly." It is the concept, endorsed by the Chairman, Joint Chiefs of Staff (CJCS), which defines the long-term goals and objectives for C4I interoperability. It provides top-level near, mid, and objective interoperability requirements. The JCS J6 integration office (J6I) is the proponent for this document. The Military Communications Electronics Board (MCEB) and the Joint Interoperability and

Engineering Organization (JIEO) are charged with overseeing the implementation of this concept. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD C3I) has also established policies that support the "C4I for the Warrior" concept.

JCS Pub 5-00.2, Joint Task Force (JTF) Planning Guidance and Procedures is a test publication that outlines the purpose, organizational structure, command responsibilities and relationships of a generic JTF. The appendices that describe the responsibilities of each of the J-staff members are extremely useful. It goes into great detail on the communications planning responsibilities of the JTF J-6.[1] It discusses interfaces into the Defense Communications System (DCS), extending World Wide Military Command and Control System (WWMCCS) circuits to the JTF and to subordinate commands, and other technical communications requirements. It assigns responsibility to the J-6 for "all C-E [Communications-Electronics] and automated information system matters."[2] Besides the WWMCCS Information Network (WIN), the only automated information system mentioned in this manual is the Joint Deployment System (JDS), and its ties to CINCs, services, and United States Transportation Command (US TRANSCOM) through the WIN. It does not address other information systems which must exchange information in support of JTF operations.

JTC3A Handbook 8000 (2nd Edition) provides useful information on basic interoperability requirements for a JTF. It provides technical information on communications and COMSEC interoperability standards and requirements, and it describes equipment used by the services which may support a JTF. It broadly describes JTF relationships, typical service C2 and connectivity requirements for JTF operations, and summarizes key portions of the JCS Pub 6-05 series (Employing Joint Tactical Communications Systems). The handbook also addresses some of the key intelligence and C2 systems found at the typical JTF level. The handbook does not really address information systems other than WWMCCS and a few intelligence systems. It provides basic data, although the new systems currently being fielded are not addressed.

JCS Pub 6-0, Doctrine for Command, Control, Communications and Computer (C4) System support to Joint Operations is a recently published doctrinal document which serves as a capstone document for the others in the series which addresses technical interoperability standards and requirements. It addresses how C4I systems support JTF operations, and it identifies interoperability and security requirements. It specifically addresses information system interoperability. Standards in this publication support the "C4I for the Warrior" concept and move interoperability requirements out of the executive level and into

identifiable standards to be achieved for C4I systems at the national, strategic, and tactical levels.

In the area of standardization, JCS Pub 6-0 calls for a minimum of interface devices or data translators, unnecessary duplication of effort across the services and requires the functional interoperability of joint and service information systems with similar uses. Technical and procedural requirements for interoperability are also mentioned. This document serves as the joint doctrinal basis for requiring the services to meet interoperability standards.

The Secure Tactical Data Network (STDN) Demonstration Report series documents a limited set of experiments which examine the joint interoperability of data communications systems and networks, and selected information systems. The first three STDNs were conducted at Ft. Gordon, GA, by personnel from the Directorate of Combat Developments (DCD) and the Battle Command Battle Lab - Ft. Gordon (BCBL(G)). STDN-4 was run by the US Navy in the pacific theater of operations. The demonstrations, conducted under the sponsorship of the JCS J-6 and validated by the Joint Interoperability Test Center (JITC), provide the reader with the status of interoperability at a given point in time, and provide recommendations on future enhancements for information systems.

Army Documents

The Army Enterprise Strategy Vision is the Army's capstone document for supporting the JCS C4I for the Warrior concept document. In fact, the JCS has formally approved the Army's Enterprise Strategy as the first service plan which fully supports the idea of "C4I for the Warrior." The strategy is a two volume document: the first volume is titled The Vision. The second volume, The Implementation Plan, will chart the course for Research and Development (R&D), future product improvement programs (PIPs), and future acquisitions and will be published by 1995. The purpose of The Vision is to explain the ten principles which will ensure that the warrior can maintain land-force dominance through proper use of force based on timely and accurate information. The Army Enterprise Strategy will

> Unify the C4I community toward a common goal; establish a structure to guide the system development process; develop economic, functional, and technical guidelines and criteria to aid resource managers in making C4I system assessments; and provide a broad systems perspective across DoD.[3]

Unlike previous vision documents from the Department of the Army's Directorate for Information Systems, Command, Control, and Communications (DISC4), this document ties the communications with the information systems for command and control (C2) and the intelligence information systems. Previously, the Program Executive Offices (PEOs) for Command and Control Systems (PEO-CCS), Intelligence and Electronic Warfare (PEO-IEW), and communications (PEO-COMM) were

allowed to develop their own requirements without top-level guidance from the Department of the Army. This document, signed by the Chief of Staff of the Army, ties Army communications and information systems into the joint perspective, and ties the idea of "C4I for the Warrior" to FM 100-5, Operations.

FM 100-5, Operations (June 1993) is the doctrinal statement of how the Army fights. For the first time, it acknowledges operations other than war. This edition increases the emphasis on joint and combined warfare by including chapters on the basic requirements for joint, combined and operations other than war within the basic document, rather than treating them as annexes. JTF operations are mentioned briefly in Chapter 4, but no treatment is given to the complex command and control requirements. Chapter 6 deals with general principles for planning and executing operations. It briefly mentions the Joint Operations Planning and Execution System (JOPES) as a means for conducting theater-strategic planning, but otherwise makes no mention of the use of automated decision aids or information systems in the planning process. Some treatment should be given to the role of automation in the planning process.

FM 100-103, Army Airspace Command and Control in a Combat Zone gives extensive treatment to the information networking required to manage Army airspace effectively. It

addresses the information required to plan, to coordinate and to execute missions.[4] However, it does not discuss what automated tools are available to support the divisional Army Airspace Command and Control (A2C2) mission. Although coordination with the Air Force is required by the Army's Battlefield Coordination Element (BCE) at the Air Operations Center (AOC), how the ATO and other information gets distributed is still undefined. Although the manual gives minimal mention of joint operations, it is useful in understanding information flow within the Army.

Books

The First Information War is a compilation of essays and articles which shows the enormous amount of communications, automation and intelligence systems which were necessary for the United States to win the Persian Gulf War in 1991. The book covers a wide range of areas--from communications on the move to strategic network access; from special intelligence communications and systems to frequency management; and from electronic warfare to the use of experimental equipment like Joint Surveillance Tracking and Reconaissance System (JSTARS). This book points out how dependent the US military has become on information. It also clearly demonstrates the value of the systems in the field when everything works. This book drives home the need for C4I interoperability by showing the amazing array of systems that are involved in the command and control and

intelligence processes. The information from each of the systems is potentially valuable to someone else in a different service. This book points out some of the key information exchanges. In the preface to the book, the editor makes a significant statement:

> if soundly grasped and properly assimilated, the principles of information warfare will lead to U.S. military forces that are not only much leaner and cheaper to field, but are still capable of effective support to the nation's goals and objectives.[5]

In a time of force reductions, interoperable C4I systems are the key to winning the nations wars.

Joint Air Operations, Pursuit of Unity in Command and Control, 1942-1991, does an excellent job in presenting the problems associated with Joint Air operations in Operation Desert Storm (ODS). One key point of this book is that problems in joint operations are not new, but we keep re-learning the same lessons. In spite of the herculean efforts taken to distribute the Air Task Order (ATO) during ODS and the ultimate successful automation of ATO distribution to the Navy, many problems remain. Basic suspicion of the other services, a lack of understanding of the other service's doctrine, and communications issues all contributed to interoperability problems. One of guidelines the authors suggest for future air operations is "The establishment of a joint air control system with its own procedures, tables of organization, and the needed hardware and software."[6]

Periodicals

Joint Tactical Communications, a Center for Army Lessons Learned (CALL) newsletter,[7] describes problems in both information management and communications. Digital datalink problems, A2C2 and ATO coordination, and coalition information exchange problems are discussed. Communications issues discussed include frequency management, data-link architecture, and range extension of communications in a highly mobile environment. It points out interoperability issues between Air Force and Army equipment, hardware and software problems, network management problems, and information system protocol limitations that existed during Operations Desert Shield and Desert Storm. These lessons learned are valuable to combat and materiel developers.

Briefings/Monographs

The Assessment of Potential for Commonality of ADP for Army and Marine Corps C2 in selected Functional Areas (Volumes 1 and 2) reviews where these two services are in the development of individual systems and looks at the system-of-systems approach that both services have taken. It emphasizes the need for interoperability between systems and makes a case for potential multi-service development of automated C2 aids based on functional analysis of the requirements. A key point in this study is that unless top-level direction is given, the services may implement data standards, formats and protocols which are incompatible.

Endnotes

1. Chairman, Joint Chiefs of Staff, Test Pub JCS Pub 5-00.2, Joint Task Force Planning Guidance and Procedures, (The Joint Chiefs of Staff, Washington D.C., June 1988), G-1 - G-A-10.

2. Test Pub JCS Pub 5-00.2, G-5.

3. Department of the Army, The Army Enterprise Strategy Vision, (HQ DA, Director for Information Systems, Command, Control, Communications and Computers (DA DISC4)), Washington D.C., July 1993), 4.

4. Department of the Army, FM 100-103, Army Airspace Command and Control in a Combat Zone, (HQ, Department of the Army, Washington D.C., October 1987), 5-1 - 5-24.

5. Alan D. Caqmpen, ed., The First Information War, (AFCEA International Press, Fairfax, VA, 1992).

6. J.A. Winnefeld, D.A. Johnson, Joint Air Operations, Pursuit of Unity in Command and Control, 1942-1991, (Naval Institute Press, Annapolis, MD, 1993).

7. Center for Army Lessons learned (CALL), Joint Tactical Communications, (US Army Combined Arms Center, Ft. Leavenworth, KS, No 92-1, Jan 1992).

CHAPTER 3

RESEARCH DESIGN

Research Approach

This chapter describes criteria and methodology for analyzing interoperability between information systems. It provides the reader with the basis to understand the analysis. The analysis in Chapter 4 is based on data obtained from field experience, combat developers, reports from JCS J-6I sponsored interoperability demonstrations, data from Program and/or Product Managers (PM) and Training and Doctrine Command (TRADOC) System Managers (TSM). This information is applied to emerging requirements from recent operations and C4I for the Warrior objectives and analyzed. The analysis of the relative interoperability of information systems is based on technical system specifications and test reports. After analyzing the levels of interoperability between information systems, the answers are applied to the requirements of JTF operations and the research question is answered in Chapter 5.

Analytical Plan

First, all available material was investigated and information relevant to the research question identified. Information came from top-level Army and Joint Staff

documents, Field Manuals, Technical Publications, other studies and monographs, Lessons Learned Reports, and Technical evaluations of equipment used for control of a JTF. Determination of whether a piece of equipment properly supports C4I of a JTF is highly subjective. Thus, interviews were conducted to gain some individual perspective on this subject, and I reviewed these for objectivity.

Information from the various documents and sources was compared to determine the relavance and accuracy of information. Matrices are used to compare the technical characteristics of the automation hardware and software to answer the supporting questions: How well do service information systems meet the objective requirements for joint interoperability established by the C4I for the Warrior concept? What levels of interoperability currently exist?

User Requirements

User requirements for automation interoperability were based on the objective requirements of C4I for the Warrior and further identified in the Global Command and Control System (GCCS) Common Operating Environment (COE). Seven of the objective user requirements as stated in C4I for the Warrior are listed along the top of Table 1. These criteria were used to evaluate the six information systems and software packages in use or about to be fielded by the

services. Information systems were evaluated on whether they comply with the objective requirements, were on track toward compliance, or were not on track.

Objective Criteria

Over the Air Updating (OTAU) is the process of automatically updating user data bases by "pushing" critical data to users based on predetermined rules. OTAU requires no intervention or action by the user. Information is delivered, processed, and the operator alerted that new data is present.

TABLE 1

USER REQUIREMENTS MATRIX

	Over the Air Update	Multi Service Fusion	Standard User Interface	Multi Level Security	Common Operating Environ	Scaleable S/W & Adaptive Commo	Access Controls by Echelon
ACCS/ STACCS							
ATCCS/ MCS							
CTAPS							
JMCIS							
FSS							
GCCS							

Multiservice Fusion is the process of receiving and integrating all-source, all-service information that comes

directly from multiple sources. The information may be provided by Compact Disk-Read Only Memory (CD-ROM), direct feed from intelligence platforms, television, another service, and so on. Blending, or fusing the data received from multiple sources will provide the user with a more realistic view of the current battlefield situation than would be available from just one source.

Standard User Interface gives the user the same look and feel even when using different software programs. Providing the user with a familiar graphic user interface (GUI) and consistent mouse and keyboard action will reduce training time. It will also relieve some user anxiety when working with new software or the systems of other services.

Multi-Level Security (MLS) provides the user with protection of data at whatever security level is authorized. Computers with MLS devices and/or operating systems will be able to process, store, transmit and receive information at multiple security levels simultaneously. Users must be able to indicate their authorized level of clearance to the information system before this system can be effective.

Common Operating Environment (COE) is essential to carrying out the other initiatives. It identifies minimum compatibility requirements, such as Portable Operating System Interface (POSIX) compliance for software that runs on UNIX operating systems, identifies minimum Random Access Memory (RAM) and hardware requirements (e.g., 32 Megabytes

(MB) Random Access Memory (RAM), 500 MB Hard Drive, Compact Disk-Read Only Memory (CD-ROM), or Microsoft Disk Operating System (MS-DOS) emulation).

Scalable Software and Adaptive Communications capabilities make the best use of the automation and communication assets available. Scalable software allows the user to run only the portions of a program that are needed to perform a particular task. Adaptive communications makes use of whatever communications means are available at any given time. These criteria allow software from across the services to run on any computer, since the system complies with the established standards.

Access controls by echelon allows the user to obtain certain types of information based on battlefield location. Some types of information are more critical than others, depending on where the user is, and designated users will get priority for that type of information. Access controls also depend on MLS, OTAU, and Multi-Service Fusion to be effective.

Hardware Interoperability

Current information system hardware specifications are compared in Table 2. This comparison is intended to determine which systems have established compliance with the common operating environment requirement, have some multi-media capability, and can connect to each other without

multiple interfaces. This comparison will be used to provide input to the User Requirements Matrix at Table 1.

Operating system requirements impact on what programs can be run on a computer. Common operating systems for government computers include Microsoft Disk Operating System (MS-DOS), Southern California Operating system version of UNIX (SCO UNIX), and the Hewlett-Packard Proprietary version of UNIX (HP UNIX or UX). Software programs must be written with a specific operating system in mind. Operating systems react differently or not at all to the same programming command, making software ineffective if a common operating environment is not established.

TABLE 2

HARDWARE INTEROPERABILITY MATRIX

	Operating System	RAM Required	Hard Disk Storage	Tape Drive Storage	CD ROM	LAN Type
ACCS/ STACCS						
ATCCS/ MCS						
CTAPS						
JMCIS						
GCCS user terminal						

RAM, Disk and Tape Drive storage capacities, and CD ROM capability effect the ability of a computer to run different types of software. Minimum requirements in these areas must be established to support scalable software operation, maintain hardware commonality, and support multi-service and multi-media information fusion.

Local Area Network (LAN) type effects the ability of computers from different services to directly connect to each other and exchange information as part of a network. The implementation of proprietary LAN hardware/software may require additional interfaces which can effect data throughput and information accessibility.

Software Interoperability

Current information system software specifications are compared in Table 3. This comparison is intended to determine which systems have established compliance with the common operating environment requirement, are capable of exporting software modules, share a standard user interface, have common database systems, have common data elements and can format messages in US Message Text Format (USMTF). This comparison provides input to the User Requirements Matrix at Table 1.

Program Language and Bindings are important in developing software that can interact with other software programs and react in an expected way. The government currently requires that new programs be written in Ada

programming language to ensure interoperability. Many software programs in fielded systems are written in other languages, but they may have Ada bindings added later on so the existing program can interact with new programs. Establishing common program bindings is important when establishing the common operating environment and developing scalable software.

TABLE 3

SOFTWARE REQUIREMENTS MATRIX

	Program Language/ Bindings	Data Base	Object Oriented/ Module Dev	POSIX Compliant	Common Data Elements	USMTF Message Capable	X-Windows/ MOTIF Compatible
ACCS/ STACCS							
ATCCS/ MCS							
CTAPS							
JMCIS							
FSS							
GCCS							

Database programs and structures are different and have not been standardized. Commonly used commercial database systems include Oracle™, Informix™, Sybase™, and dBase IV™. Each database system uses data in a different way. Some require more memory than others, and there are

versions of these database applications for different types of operating systems. The use of different database systems can severely restrict the desired multi-service fusion of information if the user wants to run programs from other services on a PC.

Object-oriented software module development supports exporting programs to other services and scalable software. Object-oriented modules stand alone and use established standards for external functions such as communications, printing, and so on. Object-oriented modules require support for standard user interfaces, common operating environment, and multi-service fusion of information.

POSIX compliance is an industry standard designed to overcome the obstacles caused by different versions of the UNIX operating system. If a software application package is designated as POSIX compliant, it should be able to run on any UNIX-based system with little difficulty.

Common data elements are necessary to properly exchange information between databases without some sort of translation device reformatting the data. Standardization of data elements may overcome some of the differences in database systems when exchanging information.

USMTF Message capability is one of the ways to exchange data between information systems. JCS has currently identified 13 different USMTF messages as the basic standard for information system interoperability.

X-Windows/MOTIF compatibility provides the standard graphic user interface for UNIX-based PCs. This provides a standard look and feel to all software packages that take advantage of X-Windows. This is a key element in establishing a standard user interface and a common operating environment.

Summary

Information gained by analysis is applied to key emerging requirements from recent operations and C4I for the Warrior objectives in Chapter 4. After the research and analysis of the levels of interoperability between information systems is completed, the answers to the requirements of JTF operations are applied and the research question is answered in Chapter 5.

CHAPTER 4

ANALYSIS

Introduction

This chapter applies the methodology for analysis described in the previous chapter. The information on hardware and software capabilities came from combat developers, reports from JCS J-6I sponsored interoperability demonstrations, and data from Program and/or Product Managers (PM) and TRADOC System Managers (TSM). This information was applied to the emerging requirements from recent operations and C4I for the Warrior objectives, and the Global Command and Control System (GCCS), which is the strategic C4I system that the tactical systems will have to interoperate with. The analysis of the relative interoperability of information systems is based on technical system specifications and demonstration reports.

User Requirements

User requirements for automation interoperability is based on the objective requirements of C4I for the Warrior. Seven of the objective user requirements as stated in C4I for the Warrior are listed along the top of Table 4. These criteria were used to evaluate the six information

systems and software packages in use or about to be fielded by the services. Information systems will be evaluated on whether they comply with the objective requirements, are on track, or are not on track.

TABLE 4

COMPLETED USER REQUIREMENTS MATRIX

	Over the Air Update	Multi Service Fusion	Standard User Interface	Multi Level Security	Common Operating Environ	Scaleable S/W & Adaptive Commo	Access Controls by Echelon
ACCS/ STACCS	YES	NO	NO	NO	H/W YES S/W NO	S/W NO Commo YES	YES-LIMITED
ATCCS/ MCS	YES	NO	NO	NO	H/W YES S/W NO	S/W NO Commo Yes	YES-LIMITED
CTAPS	YES	YES	YES	NO	YES	S/W YES Commo YES	YES-LIMITED
JMCIS	YES	YES	YES	NO	YES	S/W YES Commo Yes	YES-LIMITED
FSS	YES	YES	YES	NO	YES	S/W NO Commo Yes	NO
GCCS	YES	YES	YES	NO	YES	S/W YES Commo Yes	YES

Objective Criteria

The following information supports Table 4, the Completed User Requirements Matrix. It includes rationale for the assessment of a particular information system as supporting the C4IFTW objectives.

Over the Air Updating (OTAU)

ACCS/STACCS. Within the STACCS-unique local and wide-area networks (LANs and WANs), the STACCS system administrator establishes the logical configuration of the system. The system administrator is responsible for creating and deleting user accounts and functional user positions. Once the system is set up, automated information exchange and information updating is supported between STACCS workstations and between workstations and data entry terminals (DETs).[1] This procedure does not fully meet the intent of C4IFTW because it excludes users that are not connected to the STACCS WAN or LAN. However, it does support some movement of the STACCS user, and pushes information to the new location, once the system administrator coordinates with the LAN manger to add the moved user to the STACCS router database.

ATCCS/MCS. This system allows users to pull information from database partitions. It also supports "pushing" data through the process of establishing Standing Request for Information (SRIs) with the owner of a MCS database partition. The information designated in the SRI can be "pushed" wherever the information is needed--as long as the user is another MCS user. There are different types of information that can be "pulled" or "pushed" with the MCS System: messages (USMTF), database queries, or Force Level Control (FLC) reports.[2]

CTAPS. This system is designed to "push" data to Air Force users from a central data server. This architecture is commonly called a client-server relationship. Remote or local users are updated with information that is relevant to their position, based on rules established by the system administrator. Remote users are currently limited to dedicated, full-time connections to the CTAPS server, although the next version of software will allow connections via packet networks such as the Air Force's TASDAC system or the Army's TPN. CTAPS has a standing requirement to pass the Army's portion of the ATO to STACCS, but the Army has not yet upgraded the USMTF message parser in STACCS to a version that is compatible with the USMTF generator in CTAPS. Until the two systems are compatible, the Army will not be able to parse the ATO. STACCS can receive the ATO as an E-Mail message which is in the American Standard Codes for Information Interchange (ASCII) format. STACCS operator would have to re-enter the data into the STACCS database for the information to be useful to other users on the network.

JMCIS. The tactical air picture is one of the pieces of information that is fed into JMCIS. In this sense, JMCIS supports over-the-air update. Because of the unique requirements of the Navy afloat and ashore, JMCIS "pulls" more data than it "pushes" to other users. Senior naval officers use the two main components of JMCIS, the

strategic OSS and the tactical NTCS-A, as the way to monitor situations, receive briefings, and make informed decisions. JMCIS can "push" selected data or messages to subordinate systems and can provide automatic updating of the system once the data is received.

FSS. Secondary imagery can be either "pushed" or "pulled" from imagery servers on DSNET 1 by computers running FSS. The key to performing either operation is coordinating with the owner of the imagery server. This coordination includes being listed in the database of authorized users, obtaining the correct COMSEC equipment to either dial up the server using a STU-III secure telephone or connecting via DSNET 1 through the use of a Blacker Front End (BFE) COMSEC device. Once the user is authorized and has the correct COMSEC equipment, he may coordinate to have certain imagery automatically "pushed" to him without asking for it. The user must tell the appropriate joint intelligence center (JIC) what imagery is in the user's area of interest, and the available images will be made available. The user also has the option to "pull" image files that are resident on the server.

GCCS. It is hard to determine whether or not GCCS meets the objective over-the-air update criteria, because there is no fielded systems to evaluate. However, based on the documents available, GCCS initially will be formed from a combination of software modules from WWMCCS, CTAPS,

and JMCIS. In this case, GCCS will meet the criteria because CTAPS and JMCIS meet the requirement.

Multiservice Fusion

ACCS/STACCS. Experimentation has begun to bring a multiservice fusion capability to STACCS. These efforts include receiving the ATO and processing aircraft track data from the Navy's OSS. Neither of these capabilities are in the field, and the experiment to receive aircraft track data from OSS conducted as part of the Secure Tactical Data Network Demonstration (STDN-3) used software that is not a part of the STACCS program to accomplish the information exchange. Multiservice information may also be exchanged in USMTF form, but this is not unprocessed data directly from a source. PM STACCS is also investigating the possibility of getting data directly from WWMCCS, but this process has security implications and will not be easy to overcome (WWMCCS operates at the TOP SECRET level). With the exception of ATO interoperability with CTAPS, STACCS is not on track for compliance with C4IFTW requirements. STACCS is not fully interoperable with the ATCCS systems, much less the joint community.

ATCCS/MCS. MCS is not on track with C4IFTW requirements. Direct data feeds from intelligence platforms, other services, and so on. are not possible within the MCS system unless the data comes in the form of a USMTF message. Plans for future interoperability include

STACCS, CTAPS, JMCIS, and the Theater Automated Command and Control Information Management System (TACCIMS), which is unique to Joint Force Headquarters in Korea. Combined information system interfaces are planned for French, German and British C2 systems through the quadrilateral interface device (QUID). Although all the joint interfaces are planned, MCS is having a difficult time meeting internal Army expectations. The first external interface priority for MCS developers is STACCS. The others will be worked out once the theater-level Army headquarters can exchange information with the Corps-level Army headquarters.

CTAPS. The CTAPS software supports joint fusion requirements. Current data feeds are from Air Force sensors and aerial platforms, but because Air Force and Navy platforms can exchange data in a common data protocol, CTAPS can receive data directly from other services. Additionally, CTAPS can send and receive ATO data from JMCIS-equipped Navy Forces, because the Navy has incorporated the ATO software module from CTAPS into JMCIS. While some of the Air Force's plans are long term, CTAPS is on track.

JMCIS. The Navy's capstone system currently has achieved much data fusion, but mostly of stovepipe Navy tactical systems. As stated above, the Navy and Air Force are working closely to maximize their interoperability and enhance the opportunities for joint fusion. JMCIS also has

functional requirements to perform unit status reporting, operational and deployment planning that is currently performed within the WWMCCS system. These are long range plans, and are envisioned to be available in fiscal year (FY) 2000.

FSS. Because the standards for electronic imagery compression and file transfer format are already enforced across all services, FSS and the other imagery systems provide the highest degree of joint fusion available. Imagery which is put in National Imagery Transmission Format (NITF) can be shared by all services. Images can be "pulled" or "pushed" from imagery servers such as the Forces Command (FORSCOM) Imagery Server Host (FISH) or other imagery servers at Joint Intelligence Centers (JIC).

GCCS. This system is designed to receive information from all services to provide strategic and operational users with a common picture of the battlefield. GCCS will accomplish this by integrating software modules from the various services, giving it access to databases and information from each of the services.

Standard User Interface

All of the joint systems support a standard, commercial, graphic user interface--X Windows, and use MOTIF to provide the standard look and feel to the software. STACCS supports X-Windows, but has a unique look and feel--Vermont Views (a software package similar to X-Windows).

MCS is in the process of developing an X-Windows add-on to the current version of MCS software, but the joint standard user interface will probably not be implemented until MCS version 12 is fielded. FSS does not support X-Windows, but it supports the equivalent for MS-DOS machines--Microsoft Windows version 3.1.

Multi-Level Security (MLS)

None of the information systems have near term plans for implementing MLS. Most systems operate at a system-high level of security, usually SECRET. System-high means that the information system can contain data that is considered SECRET, and that the operator must be cleared for SECRET information, even if the operator wants to perform UNCLASSIFIED functions. The communications means used by the information system must also be capable of safeguarding the transmission of SECRET data.

Common Operating Environment (COE)

GCCS is the standard used to evaluate COE functionality because it is the objective strategic information system that tactical and operational information systems will have to interoperate with. STACCS, CTAPS, and JMCIS were evaluated by the Defense Information Systems Agency (DISA) on their ability to support the GCCS COE. According to the systems assessment for the GCCS COE,

> the selected GCCS COE should be easily enhanced to provide necessary infrastructure functionality for accommodating those mission area applications desired to be part of the GCCS but which are hosted on infrastructure functionality not available in the selected GCCS COE.[3]

In other words, the functional software from the candidate systems must be capable of running on a variety of hardware platforms. The idea behind the COE is to have established joint standards for system hardware and software, allowing the functional user programs to take advantage of a common set of well-documented core capabilities. These capabilities include message and communications services, network and workstation services, electronic map and alert services, a standard graphic user interface, and a software "tool box" which is available to assist the system manager. This idea also facilitates the separation of the database from the database management system, and move system developers towards object-oriented databases in addition to object-oriented program structure.

For the GCCS COE evaluation, DISA established a limited set of criteria for evaluation because the candidate information systems are so different, and are documented differently. Some of the criteria used in evaluating STACCS, CTAPS, and JMCIS were (1) the availability of documented Application Programming Interfaces (APIs), (2) the anticipated accommodation of standards-compliant products (government and commercial), and (3) the ease of

use of multiple vendor commercial-off-the-shelf (COTS) products for the GCCS COE.

ACCS/STACCS. The STACCS system has the potential to meet the objective COE standards. However, the current form of STACCS is not a leading candidate for incorporation into GCCs because it does not meet the three criteria above. STACCS has limited documentation of APIs, possibly due to the fact that STACCS was originally developed through the use of CINC-initiative funds in Europe, and therefore not subject to the normal Military Standard (MIL-STD) 2167A documentation requirements for software development by a recognized DoD program.

STACCS is also limited in accommodating open standards products due to the tight integration of the system software, the databases, the methods of database updating and file transfer, and the current requirement for a dedicated, closed, router and packet-switched wide area network (WAN). This tight integration between STACCS elements also limits the future enhancement of STACCS without major changes in the system architecture. In short, STACCS has potential--the system hardware supports current commercial standards (Table 5), the software standards comply with the GCCS requirements (Table 6), but the overall system design needs work before STACCS is compliant with the GCCS COE.

ATCCS/MCS. MCS, like STACCS, meets the general hardware and software (Table 6) interoperability requirements for the COE (Table 5). However, MCS is also a victim of its own design (Figure 6.) and therefore does not meet the COE requirements. In the case of MCS, this

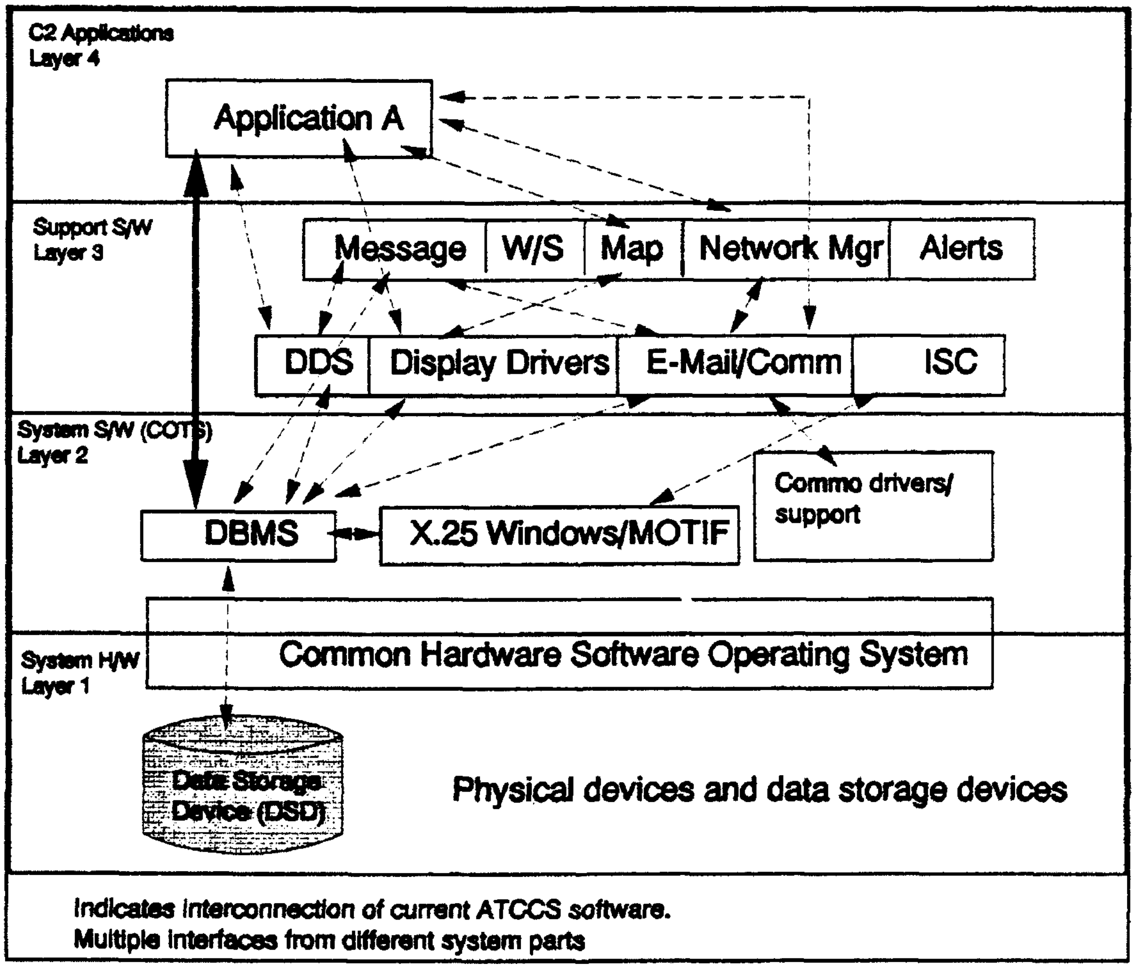

Figure 6. MCS Software Structure Today

SOURCE: Briefing, TSM-ABCS, CASS, (HQ, CAC, March 1994).

architecture is due to the fact that the software code was written at a low level to take advantage of application-specific, operating system to database management system (OS/DBMS) shortcuts and undocumented routines. While this architecture is faster and more efficient than some others, it does not support the evolution of MCS software to operate in the COE. Figure 6 shows the current MCS architecture with the implementation of the MCS common core of services, called Common ATCCS Support Software (CASS). The structure of these services is similar to, but not the same as, the GCCS COE.

CTAPS. Although CTAPS is a rapid prototype system, its use of commercial standard hardware (Table 5) and software (Table 6) that meet the COE criteria make it a leading candidate for early incorporation into GCCS. The current version of CTAPS still has to have some modification done in order to be fully compliant with the C4IFTW open standards requirements, but the system developer believes that CTAPS will be fully compliant with the open architecture and the COE requirements by March 1996.[4] The current version of CTAPS has most APIs well documented. These APIs, coupled with the high degree of modularity built into the software already, makes CTAPS well positioned to accommodate future standards. Because the software developers have taken care to separate the databases from the DBMS, and create a core of standard computer services

that is similar to that required for the COE, CTAPS is capable of setting the interoperability standards for all other information systems to meet.

JMCIS. According to the GCCS COE assessment, JMCIS is the information system that best meets objective COE criteria today.[5] Functional components of JMCIS could be incorporated into GCCS within the next year. JMCIS already runs on a variety of hardware platforms (Table 5), and incorporates modules from many different Navy systems that were originally developed as stand-alone applications. This flexibility does not mean that JMCIS meets all the COE requirements. Like CTAPS, JMCIS needs additional work in order to operate in the objective COE.

FSS. This software package is flexible, and runs under MS-DOS or MS-Windows. The software has been ported to run on UNIX-based machines as well, increasing its flexibility. Although FSS does not technically fall into the COE category, its ability to receive imagery products makes it a common system. With FSS, any personal computer (PC) can receive, store and print imagery. This capability is invaluable, wherever a warfighter is located. JMCIS is in the process of adding an imagery module to its software package. Because it is based on the same software as FSS, interoperability will be easy.

Scalable Software and Adaptive Communications

ACCS/STACCS. STACCS has a limited client-server capability, which allows some degree of software scalability. Client machines, which are usually remotely located Zenith Z-248 machines (80286 or 80386 equivalent), do not require the full load of STACCS software in order to interface with a STACCS node. However, this fact does not mean that STACCS software is scaleable. Because STACCS is such a tightly integrated series of software programs, it is not possible to load just one of the STACCS applications and run it by itself. Because database services, the user interface, communications access, database management and network management are so intertwined the user must have all of STACCS software loaded in order to use it.

STACCS does have highly adaptable communications interfaces. The access to the Wide Area Network (WAN) of communications systems by any STACCS user is determined by the system administrator. When authorized, the user has access to local LANs, the STACCS WAN, and can dial into the STACCS WAN through the use of a STU-III secure telephone and a modem. These communications means are appropriate at theater Army level. STACCS developers are investigating providing access to Combat Net Radio (CNR), which is used mainly at the tactical level.

ATCCS/MCS. Scaleable software is not supported in the MCS program. Software developers discovered that there

should have been a requirement for scaleability when they first attempted to load MCS software on the Lightweight Computer Unit (LCU) which was procured under the Common Hardware Software (CHS) contract. Due to a number of differences in hardware capabilities and operating system bios, the full MCS software could not run on another platform. Had the software been scaleable, some portions of MCS that were text, and not graphics-driven, could have been run.

MCS does have highly adaptive communications access. It supports many data protocols, some MCS-unique, and can work over secure tactical telephones, High Frequency (HF) and Very High Frequency (VHF) radios, commercial telephones and modems, and now has a newly developed interface to the tactical packet network (TPN).

CTAPS. The requirement for software scaleability is determined by CTAPS system administrator, who determines access to the separate CTAPS functional modules. Users are not required to load the entire CTAPS program, but only the portions that are appropriate. For instance, a logistics planner would have no reason to access the ATO development module, so that portion of software would not be downloaded to the user. However, the logistics user does have access to the core office automation, communications, and message preparation modules.

CTAPS also supports adaptive communications. The

basic capabilities include access to the Air Force's common-user data network, TASDAC, and point-to-point dedicated circuits between remote users and the CTAPS server. Point-to-point connections may be made through either the commercial or tactical telephone systems.

JMCIS. Because JMCIS is made up mainly of loosely connected stand alone software programs, it is possible to run portions of it without running the entire suite of programs. At the strategic level, JMCIS does not use the software packages derived from NTCS-A, but rather the appropriate software packages that make up OSS--the system designed to support shore-based operations.

JMCIS also supports a variety of communications systems--from tactical shipboard communications to strategic data networks, including DSNET 1, MILNET, and commercial telephone connections via modem. Although these communications systems are different from the Army's and sometimes use different protocols to exchange data, there are common data protocols that support interoperability.

FSS. This software package is not scalable. It is the bare minimum software required to download, store and exchange imagery with other FSS-equipped machines or imagery servers. It supports only two means of communication--packet switched networks on DSNET 1 or a similarly secured data network, and secure telephone access with a modem.

GCCS. When the candidate systems are successfully integrated under the GCCS contract, it will have the capabilities of those systems; both in software scalability and communications adaptability.

Access controls by echelon

All C2 systems have some form of access controls. In most cases, the level of access is established by the system administrator. None of the systems have a pre-determined set of rules for establishing who has access to what information. None of the systems currently meet the criteria established in chapter three. Only FSS has no access controls. FSS relies on access controls at a higher level to control access to information.

Hardware Interoperability

Information system hardware specifications are compared in Table 5. This comparison determined which systems have established compliance with the common operating environment requirement, are multi-media capable, and can connect to each other without multiple interfaces. This comparison supports the Completed User Requirements Matrix at Table 4.

Evaluated Systems

ACCS/STACCS

The STACCS system hardware is currently a combination of Army Common Hardware Software (CHS)

TABLE 5

COMPLETED HARDWARE INTEROPERABILITY MATRIX

	Operating System	RAM Required	Hard Disk Storage	Tape Drive Storage	CD ROM	LAN Type
ACCS/ STACCS	HP UX, MS-DOS 3.3 or higher	32 MB	760 MB	650 MB Magneto-Optical Disk	600 MB	802.3
ATCCS/ MCS	HP UX V 9.0, MS-DOS	16 MB	422 MB	650 MB Magneto-Optical Disk	600 MB	802.3
CTAPS	Sun UNIX	32 or 64 MB	848 MB minimum	150 MB or 1.3 GB tape dr optional	644 MB internal	802.3
JMCIS	Sun UNIX HP UX	16 MB to 64 MB	640 MB to 2.1 GB	5 GB tape dr optional	644 MB	802.3
GCCS user terminal	HP UX or SUN UNIX	64 MB min	640 MB to 2.1 GB	Unknown	644 MB	802.3

equipment, and non-developmental computer hardware built by Hewlett Packard Corporation (HP). The STACCS operating system is a proprietary form of the UNIX operating system (HP-UX). The target operating system for future versions of STACCS is the Southern California Operating System version of UNIX (SCO UNIX). SCO UNIX is generally accepted as the Army Standard for future computer operating systems. There are differences between SCO UNIX and the operating system used by joint information system developers, but these differences should not cause difficulty in loading programs

such as CTAPS on a computer that normally runs STACCS, because the operating systems are POSIX compliant. However, the STACCS common core of services are not the same as those used by joint systems, nor are they the same as the core specified in the GCCS COE. STACCS has a MS-DOS co-processor to run MS-DOS. STACCS systems in the field run MS-DOS version 3.3 or higher in order to run commercial word processing, graphics or database packages.[6]

The RAM, hard disk and tape drive storage capabilities are adequate for today's operations. However, the hardware is in need of replacement to handle future system upgrades. Projections from the STACCS program office call for replacement of the current HP hardware with Reduced Instruction Set Computers (RISC), 1 Gigabyte Hard Disk Drives (HDD) and bringing the RAM capability to 140 MB.[7]

The CD-ROM for STACCS is part of the Army Common Hardware Software (CHS) suite. However, it also has a Magneto-optical (MO) disk built to military specifications (MIL-SPEC) and is therefore different from those commercially available, and not likely to be bought by joint users. Joint systems do not list the MO disk as required hardware. It is unique to CHS, because the other systems appear to be requiring CD-ROM, and not MO disks. The CD-ROM currently reads Defense Mapping Agency (DMA) data and will be able to read CD-ROM disks from other services.

The STACCS system uses a current commercial standard Local Area Network (LAN)--802.3, or commercial ThinLAN. However, the LAN is connected to the external communications systems by a series of commercial packet routers. The implementation of routers in this system is integral to the say the databases are updated and information exchanged across the Wide Area Network (WAN). The specific implementation of routers isolates STACCS from other computers, requiring a dedicated packet network just to support STACCS. The implementation of routers is effective for the time being, where there are not many data network users in the field, but it is a future limiting factor.

ATCCS/MCS

The MCS system hardware is also Army CHS, which uses the Hewlett Packard Corporation proprietary form of UNIX (HP-UX). Like STACCS, the target operating system for future versions of MCS is SCO UNIX. This conversion from HP-UX will probably not occur until MCS version 12 goes to the field between 1996 and 1998. MCS also has a MS-DOS co-processor, which is required to run the applications under the Integrated Business Package (IBP).

The RAM available on current MCS systems is inadequate, and is one of the causes of user dissatisfaction with the software. The RAM has already been upgraded twice from the original MCS specification, but the complexity of

the software programs being run require more RAM to meet the expectations of users.[8] Hard disk and tape drive storage capabilities are adequate for today's operations. However, the hardware is in need of replacement to handle future system upgrades. The Materiel Developer for MCS, the US Army Communications and Electronics Command (USA CECOM), is in the process of procuring the next generation of CHS that MCS will run on. It is not known what that future hardware will be, so it is difficult to determine future capabilities. One version of CHS is projected to be a RISC machine, while another is projected to use a Motorola 68040 chip (equivalent to the Intel 80486 chip).

The CD-ROM and MO disks for MCS are also part of the Army Common Hardware Software (CHS) suite and have the same capabilities as the CD-ROM in the STACCS system. MCS also uses the same commercial standard LAN as STACCS--802.3, or commercial ThinLAN. However, there are plans to use a combination of 802.3 LANs and Fiber Optic cable in the field to interconnect MCS or other ATCCS devices which are located inside Standard Integrated Command Post (SICPS) shelters. This combination LAN will complicate matters in tactical command posts. ThinLAN, or 802.3 ethernet cable will have to be run to the servicing packet switch. Fiber optic cable would then link the computers within the command post (CP). Hardware interoperability within the Army should not be a

significant problem for the Army, because the basic hardware platform remains the same--CHS.

CTAPS

CTAPS hardware platform is a SPARCstation 2™, built by SUN Microsystems Corporation. The computer system uses a proprietary version of the UNIX operating system (OS) called SunOS™. This OS should not create an interoperability problem because the operating system complies with the portable operating system interface (POSIX). This compliance means that the operating system, although unique, will react in predictable ways. When software is written with POSIX compliance in mind, it will react the same way to the operating system, regardless of proprietary implementations.

The large amount of RAM available is adequate, and supports future expansion. The internal HDD, tape drive and CD-ROM, which are in wide commercial use, allow the Air Force to capitalize on commercial upgrades in the future. CTAPS also has the standard 802.3 LAN adapter and an MS-DOS emulator (not an MS-DOS co-processor).

JMCIS

JMCIS hardware is varied. The OSS software which is located at shore stations, also runs on a Sun Microsystems Corporation SPARCstation™ workstation. The portion of JMCIS that operates aboard ship, NTCS-A, runs on

ruggedized SUN™, SUN SPARC™ or Hewlett Packard 700 series™ workstations bought under the Navy's TAC-3 contract. Because of this, hardware configurations vary. As a general statement, the hardware platform is tailored to meet the needs of the ship or the shore station. The SUN equipment has far more capability than the HP, including up to 64 MB RAM, a 2.1 GB HDD, and internal CD-ROM. LAN capability is 802.3.

GCCS

GCCS is still under software development and is not fielded. The GCCS System Integration Plan calls for the GCCS software to run a variety of hardware platforms. The hardware requirements also vary from echelon to echelon. At the strategic level, GCCS hardware will consist of several servers. Hardware identified for use at this level includes the current WWMCCS Data Processing System (DPS) 8000 series servers, the SUN SPARCserver 2000™ and SUN 1000™ workstations. At the user level, the GCCS software is supposed to be capable of running on commonly found computers. Developers use the CTAPS or JMCIS hardware capabilities as the benchmark for user sysyems at remote or client locations.

Software Interoperability

Current information system software specifications is compared in Table 6. This comparison is intended to

determine which systems have established compliance with the common operating environment requirement, are capable of exporting software modules, share a standard user interface, have common database systems, have common data elements and can format messages in US Message Text Format (USMTF). This comparison will be used to support the Completed User Requirements Matrix at Table 4.

TABLE 6

COMPLETED SOFTWARE REQUIREMENTS MATRIX

	Program Language/ Bindings	Data Base	Object Oriented/ Module Dev	POSIX Compliant	Common Data Elements	USMTF Message Capable	X-Windows/ MOTIF Compatible
ACCS/ STACCS	Ada, C++ with Ada bindings	INFOR-MIX with supporting SQL	No	Yes	No. Some USMTF elemnts, but STACCS unique	Yes, but limited. USMTF ver to be used is not known	Uses X-Windows but has unique look/feel
ATCCS/ MCS	Ada, C++ with Ada bindings	INFOR-MIX	No	Yes	No. Mix of USMTF and MCS unique	Yes. Ver 11+ will use 1992 version	Ver 11+ and 12 will comply
CTAPS	Ada, C	Oracle & Sybase w/ SQL	Yes	Yes	No. AF unique	Yes. 1992 USMTF	Yes
JMCIS	Ada, C	Oracle 7 & Sybase w/ SQL	Yes	Yes	No. Navy unique	Unknown	Yes
FSS	C++	N/A	No	No	Common for imagery	N/A	No - uses MS Windows
GCCS	COBOL, GMAP, Ada, C	Oracle w/ SQL	Yes	Yes	Derived from other systems	Min 13 standard messages	Yes

Evaluated Systems

ACCS/STACCS

STACCS, which was originally developed under a CINC-US Army Europe initiative, has a combination of

programming languages. The programs are written in standard Higher Order Language (HOL), mostly in the "C+" programming language. It provides for future Ada software development, but little of the system capability is based on a programming language called Ada. STACCS provides bindings from the programs to Ada in order to meet the basic requirement for Ada standardization in DoD. Software development is unique, and includes some proprietary 4th generation language (4GL) programming as well. The product manager for STACCS (PM STACCS) is in the process of fully documenting STACCS Application Programming Interfaces (APIs).

STACCS uses a commercial relational database management system (RDBMS) called INFORMIX. INFORMIX is the same RDBMS used by MCS, but the data element structure is not the same. This structural difference creates interoperability problems, except when USMTF messages are passed. Planned enhancements to STACCS include the implementing the 13 standard USMTF messages for joint interoperability, but they are not yet part of the system.

Because STACCS was developed originally for use in Europe, it has unique data elements and structure. System designers were not constrained to any existing standard. Data queries are handled by structured query language (SQL) with a commercial standard DBMS. STACCS exchanges files by

implementing commercial and government standards such as File Transfer Protocol (FTP) and remote procedure call (RPC).

STACCS could support object-oriented software module development, but it does not do so now. One reason is because STACCS contains a series of tightly integrated software programs. It is difficult to change one program without changing parts of other programs that interface with it. This is a key flaw in the system with regards to joint interoperability. However, because STACCS is written in programming languages that support object-oriented programs, it may be easier to convert STACCS to object-oriented format than is currently thought.

STACCS only makes X-Windows available to those users directly connected on the LAN. Remote users are not supported with X-Windows. MOTIF look and feel is not emphasized (STACCS uses Vermont Views), giving STACCS a unique user interface, even when using X-Windows.

ATCCS/MCS

MCS, which began development in the late 1970s, also has a combination of programming languages. The original programs have been rewritten, and the newest additions to MCS were written in the commercial de facto standard for program writing, C and C+. Like STACCS, MCS provides for future Ada software development, but little of the system capability is based on Ada. MCS has Ada bindings

from the programs written in C+ in order to interface with Common ATCCS Support Software (CASS), which also has Ada bindings, to interface into standard communications services, database services, Graphic User Interface (GUI), and other common applications.

MCS also uses INFORMIX as its RDBMS. As stated before, the data element structure within the database is not the same as the one used by STACCS. This lack of standardization creates interoperability problems, except when USMTF messages are passed. Although MCS makes extensive use of USMTF messages and message formats, MCS has not yet implemented all 13 standard USMTF standard messages for joint interoperability yet. This slow development is due in part, to funding constraints, and partly due to the way the system was developed and the way the databases were linked to other parts of the MCS program.

MCS does not support object-oriented software module development. The operating system and database management system are optimized for the current applications in order to make them run as fast as possible on the limited RAM available. Changes in MCS program logical descriptions involves modifying and then recompiling the entire program. MCS is not currently capable of meeting the joint interoperability standards. MCS does not currently support X-Windows. A future version of MCS 10.3 will have an

X-Windows user interface, but X-Windows will not be fully implemented until version 12 is released.

CTAPS

The Air Force developed the current CTAPS software modules as a rapid prototype for test and evaluation by October 1994. The original software developers from Air Combat Command (ACC) wanted to maximize the use of existing government and commercial standards to reduce development costs. The CTAPS approach to system development requires heavy user involvement and truly embraces the evolutionary development of software that the Army should follow. The programming language used by CTAPS supports the object-oriented requirements of C4IFTW, and the use of CTAPS modules by other services when the common operating environment (COE) standard is fully implemented.

CTAPS uses two different commercial database management systems--Oracle and Sybase. Most software modules access the database through the use of Oracle, but intelligence applications require the use of Sybase. Because the databases that are resident on the system are relational, use the same data element structure, and are decoupled from the database management system (DBMS), the use of two different, proprietary, DBMSs is effective. The use of standard data elements is a lesson the Army should heed when developing future systems.

The CTAPS communications module can send E-Mail using commercial standard Transmission Control Protocol/Internet Protocol (TCP/IP), or it can generate messages for entry into AUTODIN or can some of the thirteen joint standard USMTF messages in the 1992 format version of USMTF. The CTAPS graphical user interface conforms to the commercial X-Windows standard, and uses MOTIF to provide a common look and feel across all application modules.

JMCIS

The Navy developed the current JMCIS software modules from components of the NTCS-A, OSS and other Navy information systems. The Navy wanted to maximize the use of existing government and commercial standards to reduce development costs and still meet the objective C4IFTW requirements. The programming language used by JMCIS supports object-oriented software module development and makes JMCIS a leading candidate for GCCS integration. It also complies with the currently understood requirements for the multi-service common operating environment (COE).

Like CTAPS, JMCIS uses two different commercial database management systems--Oracle™ and Sybase™. This use of two RDBMS' on the same platform is due to the quick integration of tactical and strategic information systems under the JMCIS program. In order to put functional software packages together as quickly as possible, the Navy decided to operate this way as a short term fix. Because

the resident databases use the same data element structure, the use of two different DBMSs seems to work here as well.

The JMCIS communications capabilities range from standard E-Mail, using commercial standard Transmission Control Protocol/Internet Protocol (TCP/IP), to tactical data link 11 or 14, STU-III secure telephone, or it can send or receive AUTODIN messages. The JMCIS GUI uses the commercial X-Windows standard, and uses MOTIF to provide a common look and feel across all application modules in accordance with the DoD style guide.

GCCS

As an objective system, GCCS will meet the objective software requirements. The other systems (STACCS, CTAPS and JMCIS will be measured against the GCCS standards.

Current Information System Interoperability

In addition to the technical hardware and software capabilities of the current information systems, it is important to assess where they are in achieving information exchange interoperability. For the purpose of this investigation, information systems can achieve interoperability in information exchange two way--through application interoperability or basic E-Mail type interoperability. The key to application interoperability is the ability of one software package or system to exchange information or data with a different system in a way that

makes the information immediately useable by the receiving system. This process may result in database updates, display screen updates, and operator alerts to new information. Basic interoperability is the ability of an information system to read and display data in American Standard Code for Information Interchange (ASCII) format. ASCII File transfer is the most common form of interoperability today. Electronic Mail (E-MAIL) systems commonly use this standard. ASCII files usually contain free text information, and cannot be used to automatically update databases, screens, or provide operator alert messages.

C2 System Interoperability

Information on current demonstrated Command and Control system interoperability capabilities is taken from the Secure Tactical Data Network (STDN-3) Demonstration Report, dated 19 April 1993. The configuration for STDN-3 participants in the C2 application is given in Figure 7. The major participants in the C2 application included NAVFOR systems Unified Build Two (UB2). UB2 is one of the basic elements in the OSS system (running on the Joint Over the Horizon Targeting System (JOTS-II)hardware). A conceptual commander's system called the Flyaway Laptop, STACCS and MCS, and CINC systems OSS (w/JOTS-II) and Radiant Mercury were involved in the experiment. Radiant Mercury is a prototype software and hardware package which sanitizes and

downgrades the classification of message traffic based on certain parameters.

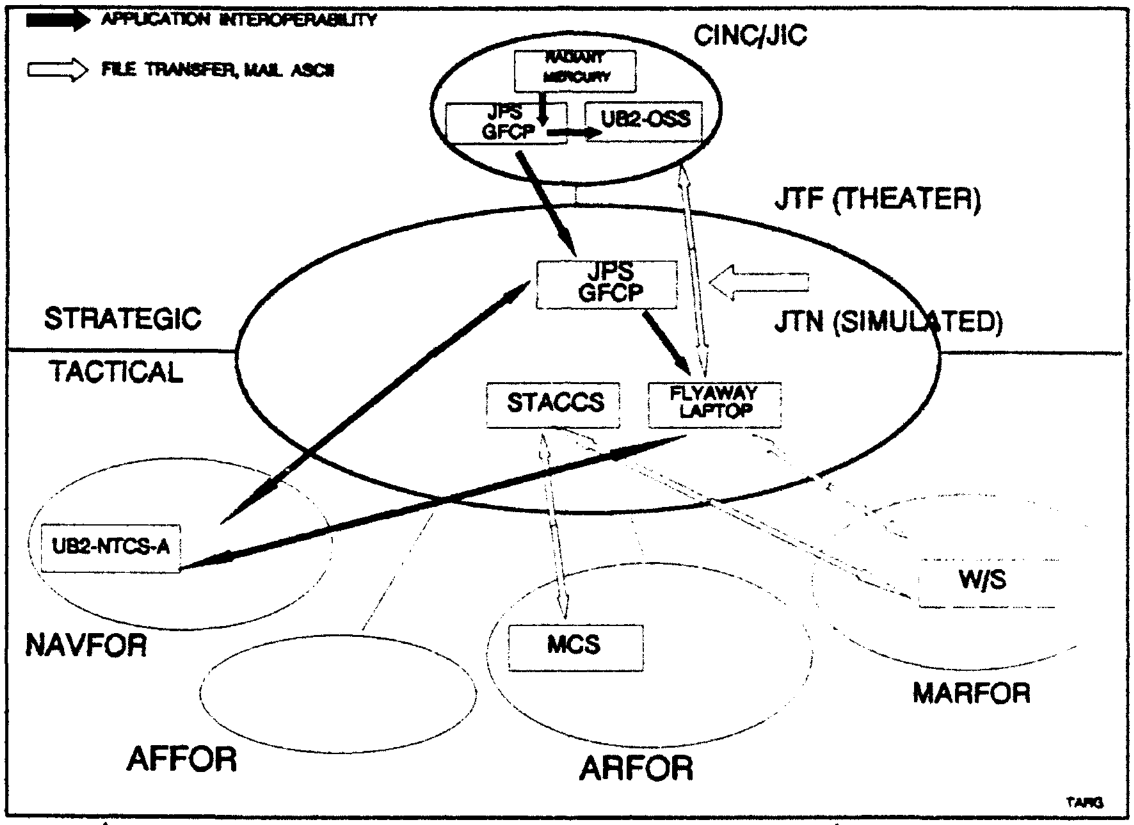

Figure 7. Command and Control Information Exchange

SOURCE: BCBL - Ft. Gordon, <u>STDN-3 Demonstration Report</u>, (Ft. Gordon, GA, April 1993).

Each of the systems involved coordinated the data exchanges with other C4I systems at random times according to their own localized demonstrations within the overall STDN-3. The essential objectives of this application were met by performing discrete message exchanges between the

systems listed, in small periods of time, so they were repeatable in a short (5-15 minutes) demonstration. Conceptually, the goal of exchanging C2 information included connectivity, USMTF message transfer and overall situational awareness afforded the JTF commander by C4I systems present at the JTF and at MARFOR, ARFOR, NAVFOR, AFOR.

STDN-3 provided the opportunities for information exchange between information system developers, and variations on these experiments were attempted. The Command and Control (C2) application experiment was focused on both a limited set of USMTF messages as well as on the overall capability provided by the C4I systems using the strategic and tactical networks. USMTF message handling between C4I systems was demonstrated in all of the above applications, and in some cases, the same messages were used. C2 messages exchanged were generated by the Joint Processing System (JPS), Radiant Mercury, and by personnel at Fort Gordon, GA, Battle Lab.

As Figure 7 clearly shows, there is little interoperability between dissimilar information systems. The Navy systems, with common software and hardware systems, and tied together by the UB2 functional software core, achieved application interoperability. Messages were exchanged with all other information systems through the use of ASCII file transfer or simple E-Mail.

Application interoperability was not possible between the two Army information systems examined, STACCS and MCS. Because messages external to MCS require USMTF format in order to fill the user database, application interoperability with STACCS was not possible. The version of STACCS evaluated had no USMTF capability (send or receive). The interoperability demonstrated by STACCS was the same minimal level for MCS and any other stand alone PC. At the conclusion of the C2 application demonstration, the Battle Lab staff reached the conclusion that a minimum set of USMTF messages is required for all levels of interoperability, and that a data translator of some sort must be used to overcome database standardization problems in the near term.

ATO Exchange

Information on current Air Task Order (ATO) interoperability capabilities is taken from the Secure Tactical Data Network (STDN-3) Demonstration Report, dated 19 April 1993. The STDN-3 Demonstration Plan identified five demonstration objectives for ATO dissemination. During STDN-3, the Battle Lab configuration and attending personnel afforded the opportunity to conduct five additional demonstrations. STDN-3 demonstrated the dissemination of Air Tasking Orders (ATOs) from the JFACC to the JTF, the CINC/JIC, and to the Force level systems, using the TPN, point-to-point connectivity (STU-III), strategic networking

(MILNET), and horizontal connectivity (component to component). Figure 8 shows the ATO dissemination flow demonstration during STDN-3.

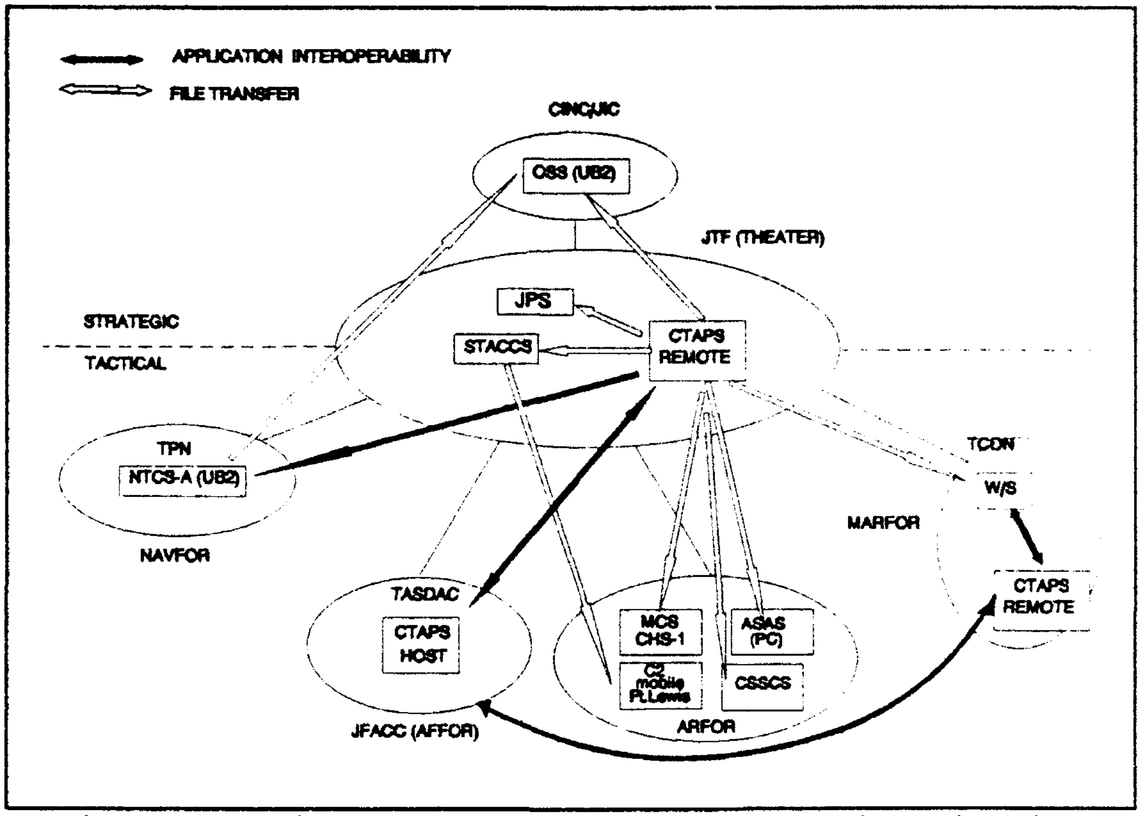

Figure 8. Air Tasking Order Functional Dissemination

SOURCE: BCBL - Ft. Gordon, STDN-3 Demonstration Report, (Ft. Gordon, GA, April 1993).

The ATO was generated by the CTAPS Host at the Air Operations Center (AOC) at MacDill, AFB and sent to the CTAPS Remote at the JTF at Fort Gordon, Georgia. The CTAPS Remote then disseminated the ATO to other systems in the Tactical Packet Network and elsewhere. Ten different sub-

demonstrations were performed. In all these demonstrations, application interoperability was achieved only where CTAPS components were present. When the ATO was sent to MCS or STACCS, it had to be sent as an ASCII file. Even though the approved method of transferring the ATO from the Air Force to the Army is via USMTF message, neither STACCS or MCS could receive and parse the USMTF messages generated by the CTAPS software. This interoperability problem is due to the use of more current USMTF format messages in CTAPS than in MCS. MCS has not yet added the correct USMTF message sets to its operational software to receive and process the ATO automatically upon receipt. STACCS did not have a USMTF capability at the time of the demonstration.

Imagery Exchange

Information on imagery exchange and interoperability is taken from the Secure Tactical Data Network (STDN-3) Demonstration Report, dated 19 April 1993. The STDN-3 imagery application demonstration was divided into two phases. The first phase was the unclassified and local demonstration of imagery capabilities using the TPN and other unclassified networks. This first phase was informal, and was performed by cooperation between participants at random times. The second phase of the experiment used DSNET1 connectivity, and was dedicated to a limited number of participants for three days. Army Space Program Office, DISA, the Naval Intelligence Center (NIC),

and the Forces Command (FORSCOM) Automated Imagery Support Agency (FAISA) at Fort Bragg cooperated in a well-defined script with clear objectives for the three-day period. Information flow for the overall architecture is provided in Figure 9.

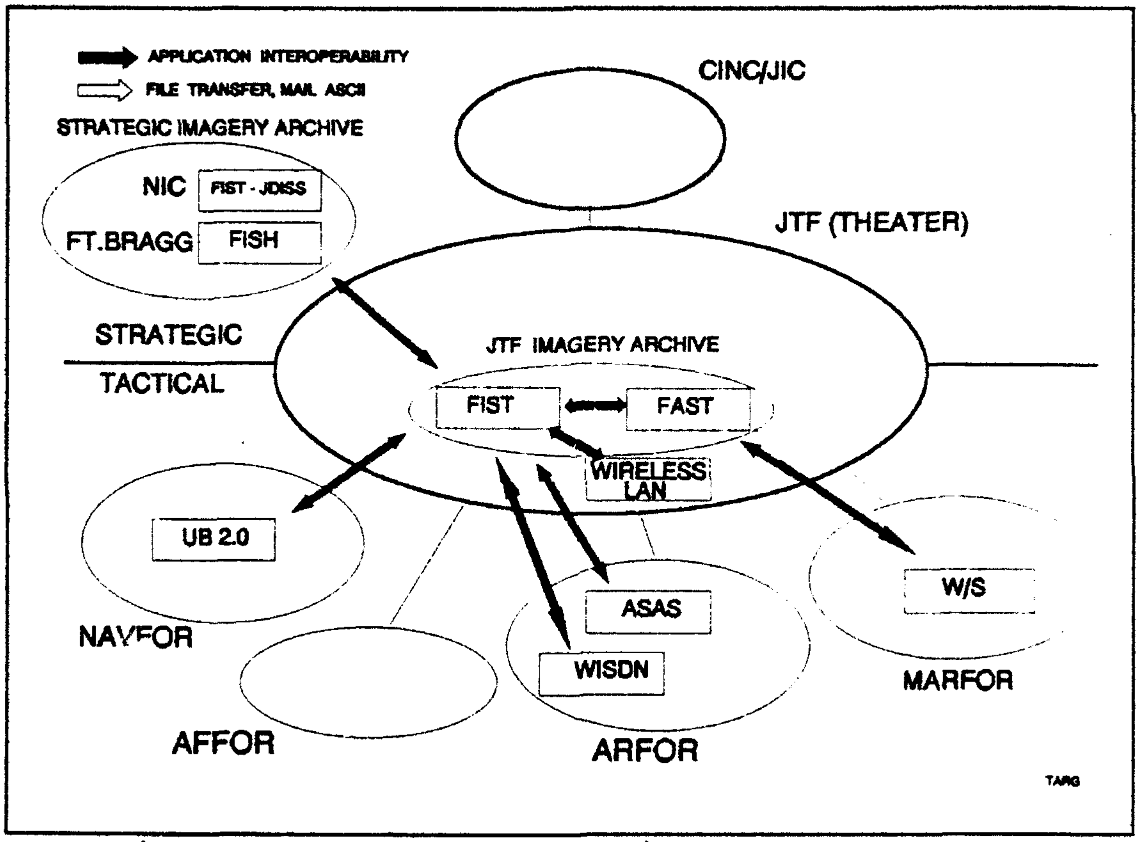

Figure 9. Overall Information Flow for Imagery

SOURCE: BCBL - Ft. Gordon, STDN-3 Demonstration Report, (Ft. Gordon, GA, April 1993).

To demonstrate a hierarchical imagery dissemination architecture, participating imagery systems were structured to serve as imagery archives at each echelon of the

architecture. The 18th Airborne Corps imagery server (FISH) simulated the strategic imagery archive, the FAST (Forward Area SIDS and TRE) and FIST (Fleet Imagery Support Terminal) served as the deployed JTF imagery archive, the ASAS and Wireless Integrated Services Digital Network (WISDN) terminals served as the ARFOR imagery archive, and a DOS terminal on TCDN served as the MARFOR imagery archive. Imagery products were passed from layer to layer in the architecture.

Imagery exchange was by far the most successful demonstration of interoperability during STDN-3. The imagery platform from each of the services was able to exchange and store images with its counterparts. This is due to the fact that a common set of software and data protocol standards was implemented by all services. This interoperability was tested before STDN-3, and was certified by the Joint Interoperability Test Center (JITC) at Ft. Huachuca, AZ. The success of the imagery exchange proves the point that a common set of software is needed for future interoperability, and all services must meet the standard.

Endnotes

1. USACECOM, Standard Theater Army Command and Control System (STACCS) System Specification Version 1.1/As Built, (USACECOM, Ft. Monmouth, NJ, October 1993), 50.

2. Project Manager for Operations Tactical Data Systems, Army Tactical Command and Control System (ATCCS) System/Segment for the Maneuver Control System (MCS) version 12, (USACECOM, Ft. Monmouth, NJ, November 1993), 3-259.

3. Defense Information Systems Organization, GCCS Common Operating Environment, (Reston, VA, December 1993), A-8.

4. ACC, Contingency TACS Automated Planning System Briefing to Combined Arms Center, (Ft. Leavenworth, KS, 1 March 94).

5. Defense Information Systems Organization, GCCS Common Operating Environment, (Reston, VA, December 1993), A-10.

6. USACECOM, Standard Theater Army Command and Control System (STACCS) System Specification Version 1.1/As Built, (USACECOM, Ft. Monmouth, NJ, October 1993).

7. TSM-STACCS, Briefing on STACCS Enhancements, (Ft. Monmouth NJ, PEO-CCS, 1994).

8. Discussion of MCS with MAJ Gary Nicholas, Chief, Tactical Automated Systems Branch, Materiel Requirements Division, Directorate of Combat Developments, Ft. Gordon, GA, 21 June 1993.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

As Chapter 4 has shown, there are many challenges and obstacles to overcome in order to provide interoperable information system support to an Army-led Joint Task Force (JTF). Information systems interoperability is possible with current systems, but the status quo will not support future Army-led JTF missions.

Current Interoperability

There is much work to be done by the Army to meet the C4IFTW requirements and to implement the Army Enterprise Strategy. The Army must integrate its battlefield digitization efforts with those of the other services to make the most effective use of research and development dollars in today's fiscally constrained environment.

There is basic interoperability between the services for C2, ATO and imagery dissemination. The analysis of the interoperability demonstrations in Chapter 4 indicates that it is possible to exchange information in a way that supports the current needs of the JTF warfighter. However, receiving and reading ASCII files that contain C2

and ATO information and then re-entering the information into a database is awkward at best. Under today's interoperability constraints, this procedure must be followed in order to provide other users with the information in a meaningful way.

Imagery dissemination demonstrates the best degree of interoperability. The standards for transmitting, receiving, interpreting and reconstructing the image at the receiving end are firmly established in the joint community, and are enforced. The requirement for JITC to certify all new applications that process imagery for compliance with NITF standards is an excellent one. This certification process should be expanded to include the C2 and ATO areas as well.

It appears that the Army is in the worst shape of all with regards to joint interoperability. The Army has invested sizeable amounts of money in developing ACCS/STACCS and ATCCS/MCS. It appears the Army did not build joint interoperability into its systems from the start. The Army may be required to accept information systems developed by the other services as joint standards.

Joint interoperability will not be effectively achieved if the Army continues on its present development course with STACCS and MCS. The Army must change its software development strategy to take advantage of software products developed by other services. An immediate fix to

allow some increased degree of interoperability between C2 systems is the use of a translator like the Joint Universal Data Interpreter (JUDI). This translator will pave the way for future interoperability (Figure 10).

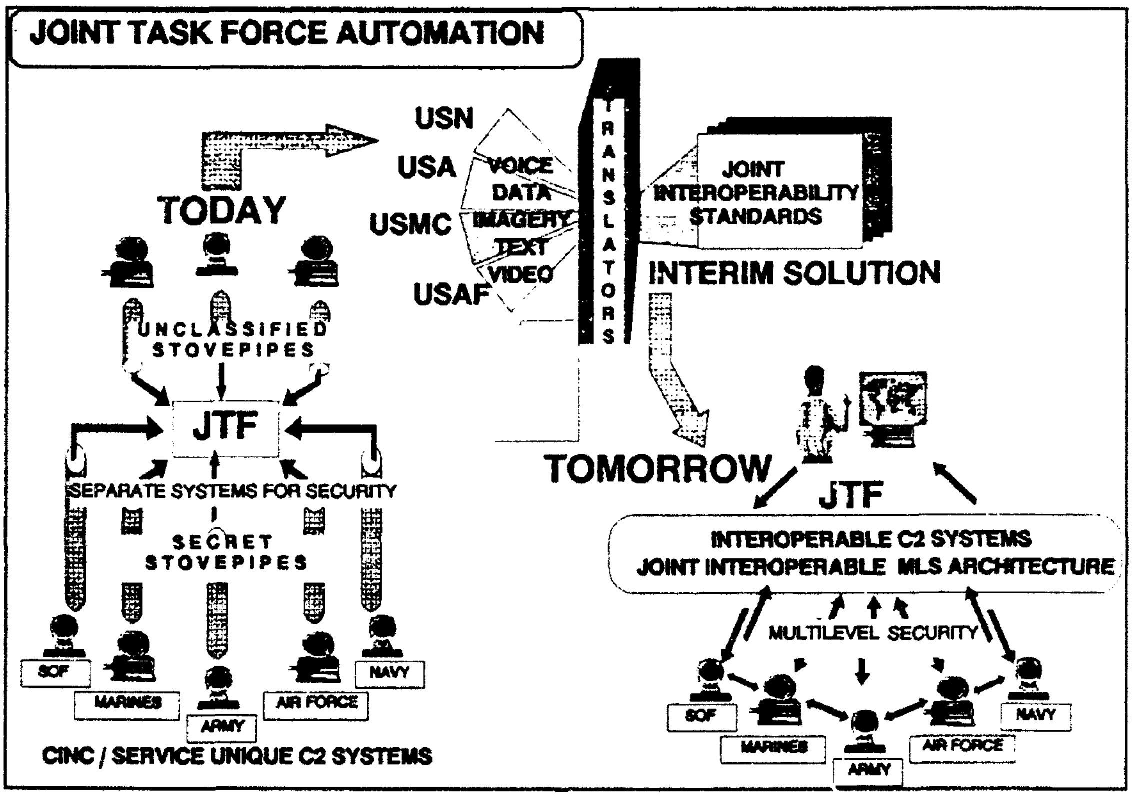

Figure 10. Migration path for C4I Systems

SOURCE: JCS J6I, C4I For the Warrior, (JCS J-6, 1993),(Modified by the Author).

Hardware Interoperability

Hardware interoperability is almost achieved. The use of existing government and commercial standard hardware has simplified this task. General trends in hardware appear

to be increased amount of RAM, a form of POSIX-compliant UNIX operating system, large hard disk and tape drive storage systems for data, and the use of CD-ROM drives for program and map data storage.

Software Interoperability

The basic tools are available to create software interoperability. The Air Force and the Navy appear to be well on their way to meeting joint standards. Their object-oriented approach to software modules dovetails nicely with the joint initiatives to establish a common operating environment (COE). Unfortunately each of the services uses their version of the COE to support service-unique user applications. The Navy and Air Force do not use the same COE. The Army also has its service-unique COE, but software developers are not developing stand-alone modules for C2 or other applications yet.

Providing Interoperable C4I Systems

There are several key elements in developing interoperable information systems. Three of the most critical interoperable elements are as follows: optimizing data for transmission between machines; standardizing data elements between services; and developing modular, object-oriented programs which can be run regardless of the computer platform. To date, the Army's attempts at digitizing the battlefield have been limited to automating

the current manual C2 and logistics functions--just do the job faster by using computers. The Army must go beyond doing the same jobs faster and make a revolutionary change in the way it develops information systems.

Optimizing Data for Transmission

One of the fundamental misconceptions in the development of current information systems is that machines use data in the same way that humans do. This is not true. Information exchange must be optimized for machine-to-machine interface, and database-to-database interoperability. For instance, users of C4I systems don't need to send United States Message Text Format (USMTF) messages between machines--they can just send bits of information, or Bit Oriented Messages (BOM) that will translate into meaningful information once received at the distant end. System developers must overcome the phobia of being able to read the message manually as a backup. The key to using digital information is optimizing the data for transmission on digital communications paths for reception by computers, and being able to send the data by different means to remain flexible in a tactical environment.

Standardized Data Elements

Standardizing data elements is another component in developing joint interoperability. The Army cannot send BOM messages or run modular software packages developed by

different services if the services cannot agree what the different data elements mean. A method to establish data definitions might involve giving each service proponency for what it does best: the Army establishes the land component data dictionary; the Navy develops a dictionary for sea operations; the Marines develop a data dictionary for amphibious operations; and the Air Force handles aerospace operations. Because of overlap in each area, services must work together in standardizing data elements.

Developing Object-Oriented Programs

The Army needs to reevaluate the current information system architecture. The Navy and Air Force are developing C4I systems which are interoperable through implementation of a core of standard computer services that are present on generic computer platforms and are compliant with joint guidelines. On the other hand, the Army is still developing closed-architecture systems such as the Maneuver Control System (MCS) and the Standard Theater Army Command and Control System (STACCS) which have similar, but not compatible, core capabilities. The Army must develop the next generation of information systems based on modular, object-oriented programming principles, using rapid software prototyping to get early feedback from the user. Databases, network and user services, and communications support for Army information systems should be decoupled from the user applications in a manner that better supports joint

interoperability. The Army needs to conform to the joint requirements for interoperability now, and not wait until later to add some interoperability module.

Objective Requirements

In addition to the hardware and software interoperability, Multi-Level Security (MLS) is arguably the most important objective requirement for all the services to achieve. None of the existing systems are implementing MLS in the near term. MLS technology is still developing and is very expensive to implement. Additionally, NSA has not determined which MLS system will become the DoD standard. All of the objective systems have plans to incorporate MLS technology in the future, because single-level security measures will not support the needs of future warfighters. Implementing MLS technology must be done as a joint effort which includes NSA.

Today's warfighter is limited in his battlefield movement by different communications security (COMSEC) devices, keylists, codewords, and so on. Implementing MLS will "provide the warfighter the ability to access and exchange information at needed levels of classification using a single C4I system."[1] Single-level security is cumbersome, and until recently, technically infeasible. Multi-Level Security technology will enable the Army to adopt commercial standards for tactical systems and achieve the goals of the C4IFTW concept.

Given C4IFTW's requirement to be able to "plug in" anywhere in the world, "reach back" to CONUS, and "pull" required information, MLS must be embedded in the appropriate user-owned and operated communications and information systems. These systems include cellular and wire-connected telephones, computers, multi-band radios, future electronic ID Cards/Tags, and even some weapons and sensors. Implementing MLS in these systems will allow secure exchange of information within the Army and between joint forces at all levels from squad to theater command with minimal difficulties. Embedding MLS in user devices will also facilitate the change in the development of military communications systems.

Digitizing the Battlefield

The Army is involved in an extensive effort to digitize the battlefield. Digitizing the battlefield offers a way to take advantage of emerging technology to improve the Army's warfighting capabilities. The digitized battlefield encompasses the use of digital maps in command centers, digital communications at all echelons, providing imagery in moving tanks, using Electronic Mail (E-Mail) to pass orders, maintaining direct sensor-to-shooter data links, using the global infosphere to pass data to strategic echelons--truly digitizing the battlefield means all this and more. Because the Army's digitization of the battlefield touches virtually every weapons system, command

and control (C2), intelligence and logistics system, the Army's initiatives must be tied to joint efforts to standardize command, control, communications, computers and intelligence (C4I) systems.

A fully digitized battlefield requires information and communications systems that are interoperable between the services at various command echelons. It also means providing information to the warfighter when and where required--regardless of service affiliation. General Colin Powell summed up the Department of Defense's (DoD's) real mission in digitizing the battlefield when he told the Senate Armed Services Committee that the services must take

> ... a total look at the communications and intelligence systems that we are purchasing for the future to make sure that they are interoperable...so every service can talk to every other service and so every unit on the battlefield can talk to every other unit on the battlefield.[2]

As the Army begins a paradigm shift--CONUS-based force projection operations in a joint environment[3]--the Army has the opportunity to shape the joint digitized battlefield of the future. Although there are many near- and mid-term fixes that the Army must implement during the digitization process, senior leaders must keep in mind that there are four basic elements which support digitizing the battlefield, future joint interoperability and Army force projection. These first of these "drivers" is leveraging commercial technology; second, the use of space-based

systems to support the digital battlefield; third, implementing Multi-Level Security (MLS); and finally, providing joint C4I system interoperability. The Army must pursue its long-term digitization efforts with these "drivers" in mind and address them in the next five to seven years to achieve joint C4I interoperability on the digitized battlefield in the 21st century.

Force Projection Requirements

Implementing the force projection paradigm shift together with battlefield digitization will be a costly effort. Instead of relying on an established in-theater communications and command and control infrastructure, force projection operations will require US forces to move rapidly to a remote area of operations on short notice. This area of operations may or may not have an established communications infrastructure. The JTF command structure will likely be put together from various service components around the world, as was done in Somalia. The JTF commander will require secure, flexible, communications enroute and during initial entry operations. Once the JTF is in theater, the deployed force must be able to access US commercial and government communications systems for voice, data, and message traffic--the global infosphere--through available military and host-nation communications support. The current family of Army command and control systems do not support this requirement.

How do we get there from here?

The Army and DoD must always remember to focus on providing support to the warfighters. The objective of DoD's combined effort is a seamless, global infosphere that combat forces, intelligence, and combat service support forces can plug into anytime, anyplace. Without this vision, the services will be where the Army is now--chasing technology a piece at a time. The Army must actively pursue joint initiatives, and lead wherever possible because the Army will commit the bulk of forces to most ground operations when a JTF is deployed. If the Army does not volunteer to lead the standardization effort, it will be put into the position of being forced to accept information or communications systems tailored to meet the other services' needs.

The Army cannot afford to digitize its part of the battlefield alone. The joint staff must be the honest broker/integrator which sets and enforces the standards for interoperability by controlling the funds for both communications and information systems, including data protocols, message text formats, and electronic map graphics. Standardization will reduce the communications and C2 problems encountered when putting a JTF together on short notice, such as occurred in Somalia. Obviously, the Joint Staff cannot oversee all details of the services'

modernization programs, so a policy of centralized planning and decentralized execution must be implemented.

Recommendations

The Army must modernize its developmental approach to information systems and software in general. It is appropriate to send Army software developers to visit Air Force and Navy information system developers to learn some of the methods that allow the Air Force and Navy to rapidly prototype systems and receive good feedback from the user on system functionality. It is also important for the Army to take advantage of what the other services have done in the area of establishing a common core of computer services and supporting the joint COE concept. If the Army takes advantage of the COE, system programmers can truly begin to develop scalable software, so users can load just the portion of the C4I program that is required.

The easy part of this recommendation is borrowing COE software from the other services. The difficult part is overcoming bureaucratic obstacles within the materiel development community, and take advantage of software that is "not invented here." Once the Army accepts the joint standards for COE, then the program managers can re-engineer their systems to take advantage of the COE and C4IFTW standards, and give the JTF commander software packages that can be tailored to his needs. It is conceivable to have portions of STACCS, CTAPS, FSS and JMCIS all loaded on the

same high-capacity computer at the JTF headquarters, receiving information feeds from each service, and keeping the JTF commander updated on the situation in an apparently effortless way. Each of the software packages would be capable of taking advantage of common computer services and interfaces and reducing the service-unique aspects of information systems and data exchange. If the data elements used by each of the information systems were standardized, data translators between systems would not be needed.

The acceptance of the joint COE will force information system software recoding to be done throughout the Army. While this is not cheap in the short term, it is in the Army's long term interests because it will decouple the databases from the DBMS, require fully documented APIs with no undocumented shortcuts, and allow the software to be run on a different operating system that meets the COE standards. Additionally, the rewrite of software code into object-oriented programming must be done at a high level--this may require a 50% rewrite in some cases. Programmers must take advantage of commercial standards for programming, graphic user interfaces, file transfer, and government standards for imagery transfer and storage, maps, and other evolving standards.

By allowing the common operating environment developers to maintain the appropriate modules, all the service program developer must do is maintain the standard

interface into the COE (Figure 11). This way, if the joint COE configuration manager decides to change the graphic user interface (GUI), the service software designer doesn't have to make any changes in software--just load the new GUI module on to the machine. The Army can take advantage of updates to commercial or standard programs and libraries and

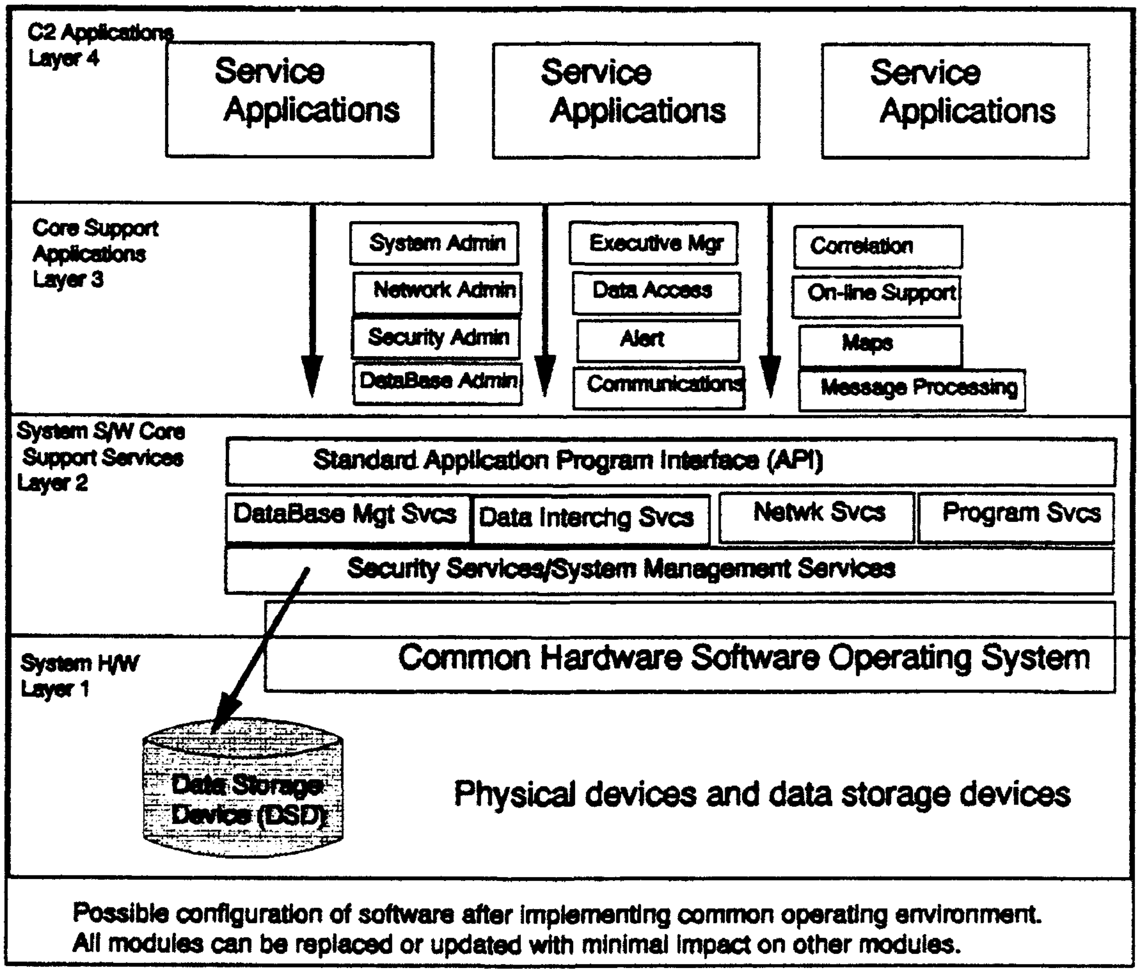

Figure 11. Possible Software COE Structure

SOURCE: Briefing, HQ, ACC, CTAPS Migration Strategy, (HQ, ACC, March 1994), (Modified by author).

incur little cost. Information system hardware must also be continuously updated in order to take advantage of technology insertion.

Advanced hardware will provide the speed that will support object-oriented programming and databases. Relational databases that are in use today are fine for data base comparisons and linked files. In the future, the databases will need to become more flexible and capable of receiving and storing video, still imagery, voice, and so on. Databases must become object-oriented along with the functional software modules. If the database were truly object-oriented, it would hold abstract data types, not just data elements. The database could contain text, voice, imagery, data, or almost any data format that could be produced by the information systems--as long as the data was standard.

Summary

In order to digitize the battlefield, the Army's senior leaders must put the pieces of the puzzle together and ensure that all concerned appreciate the vision of the future battlefield. The Army must move beyond the idea that digitization of the battlefield is at brigade-level and below, and develop information and communications systems that are interoperable between the services. Supporting the warfighter can be accomplished by identifying our objective joint C4I requirements, and setting goals for future C4I

systems that are realistic. These systems must provide the necessary information to the warfighter in a timely and meaningful way anywhere on the battlefield.

The Army has accomplished the first part of this mission--the Army's objective C4I requirements are defined in The Army Enterprise Vision. Judicious funding of Army and joint programs which will allow the Army to sustain and protect the force, win the information war, and dominate the battlefield is also required. The Army's digitization process can be the framework for conquering the challenges of joint C4I in a force projection environment if it leverages commercial technology and is in accordance with joint standards for information system design and implementation. The recommendations in this study are doable, provided funds are made available. If changes to Army information system development and design are not instituted, the success of an Army-led JTF could be sacrificed.

Areas for Further Study

The interoperability of Joint Special Operations Task Force (JSOTF), intelligence and logistics information systems should be investigated, and evaluated along the same criteria as the systems in this study. The communications that support a JTF should also be examined, with special emphasis on wide area network (WAN) management, LAN management, and service-unique communications

interoperability issues that have grown from the Army's fielding of Mobile Subscriber Equipment (MSE) and the modification of Army Echelons Above Corps (EAC) switchboards. Other issues related to digitizing the battlefield, and information system interoperability include the areas of Multi-Level Security (MLS) and increased use of satellites to support force projection operations by joint forces.

Endnotes

1. Office of the Secretary of the Army, The Army Enterprise Vision, (Director of Information Systems for Command, Control, Communications and Computers (DISC4)), Washington D.C., July 1993), 8.

2. Chairman, Joint Chiefs of Staff, Statement to the Senate Armed Services Committee, (Washington D.C., 10 March 1992).

3. Department of the Army, FM 100-5, Operations, (Headquarters, Department of the Army, June 1993), 2-2.

APPENDIX A

DEFINITION OF TERMS

Combatant Command. AFSC Pub 1, The Joint Staff Officer's Guide, defines Combatant Command (COCOM) as nontransferable command authority established by title 10, United States Code, section 164, exercised only by commanders of unified or specified combatant commands. Combatant Command (command authority) is the authority of a Combatant Commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command.

Joint Task Force (JTF). AFSC Pub 1, The Joint Staff Officer's Guide, defines a JTF as a force composed of assigned or attached elements of the Army, the Navy and/or the Marine Corps, and the Air Force, or two or more of these Services, that is constituted by the Secretary of Defense or by the commander of a unified or specified command, subordinate unified command, or an existing joint task force.

Command and Control. JCS Publication 1-02, The DOD Dictionary of Military and Associated Terms, defines Command and Control (C2) as "Exercise of authority and direction by a properly designated commander over assigned forces, in the accomplishment of the mission." The Army generally includes the supporting communications systems[1] in its definition of C2, and discusses C2 as an operational process. The Army does not define C4I systems, but assumes them as part of the C2 definition. C4I will be used when discussing the overall system architecture because the long term strategy for interoperability is called "C4I for the Warrior."

Information Systems. A term which generically describes automation hardware and software which supports information distribution, processing, and presentation. Any automated C2 or Intelligence system may be considered an information system.

Interoperability. The "ability of systems, units, or forces to provide services to and accept services from other systems, units or forces and to use the exchanged services to enable them to operate effectively."[2]

Application Interoperability. The ability of one software package or system to exchange information or data with a different system in a way that makes the information useable and understandable by the receiving system. This results in automated use of the information as well as exchange. Databases are filled with new information, display screens updated, and the operator is usually alerted that new information is available.

Data Format Interoperability. The ability of dissimilar information systems to read data stored in a standardized way. The information may or may not be directly translatable into a database, depending on the ability of the receiving system to parse the information.

Basic interoperability. The ability of an information system to read and display data which is in American Standard Code for Information Interchange (ASCII) format. ASCII File transfer is the most common form of interoperability today. Electronic Mail (E-MAIL) systems commonly use this standard. ASCII files usually contain free text information, and cannot be used to directly fill databases.

Endnotes

1. Department of the Army, FM 101-5-1, Operational Terms and Symbols, (US Government Printing Office, Washington D.C., October 1985), 1-16 & 1-17.

2. FM 101-5-1, p. 1-39.

APPENDIX B

DEFINITION OF EQUIPMENT

Army Tactical Packet Network (TPN)

The MSE packet overlay is fielded to Echelons Corps and Below (ECB) units, including the contingency corps. The TRI-TAC packet overlay to AN/TTC-39D switches began fielding in September 1993. Echelons Above Corps (EAC) contingency communications units will be fielded all the components of the TPN by May 1994. The TPN-DDN interface concept and physical connection is a vital part of both the EAC and ECB packet overlays and will be included as part of the fielded system. Although current doctrine calls for the TPN to support SECRET information systems, the TPN can support either UNCLASSIFIED or SECRET users--depending on which strategic network the TPN is connected with(UNCLASSIFIED MILNET or SECRET DSNET 1).

A Packet Network Management Center (PNMC) is provided for management of the TPN. At the Corps and Division level, the PNMC is located inside the Mobile Subscriber Equipment (MSE) System Control Center (SCC) shelter. The PNMC is allocated two per Corps and one per Division. At Echelons Above Corps (EAC), the PNMC is a stand-alone workstation that is mounted in transit cases. It is allocated one per EAC Signal Brigade. The PNMC software is based on current DDN management software. The capabilities of the PNMC are the same at all echelons.

The PNMC monitors packet network connectivity and status of packet switches and gateways within its network. The PNMC is also capable of monitoring designated computers connected to the network(commonly called high priority hosts) through interaction with the Tactical Name Server (TNS). It maintains network databases and can isolate faults in the network. A graphical user interface (GUI) will make the system more user friendly than the current DDN software. PNMC capabilities include the following: Forward Error Correction (FEC) on/off selection for links; receiving alarms for events affecting network service; receiving event reports such as new packet switches entering the network, node up/down status, and exceeded error thresholds for trunk

lines. The PNMC can also download packet switch and gateway configuration parameters.

The TPN security architecture is based on the combination of bulk encryption of the TRI-TAC and MSE systems by communications security (COMSEC) devices and physical security of the local coax cables and wire lines. This combination is sufficient to qualify the system to operate in the SECRET System High Mode. Army Tactical Command and Control System (ATCCS) computer systems, which process and distribute information at the SECRET level, will have no additional security requirements or devices imposed upon them because of TPN's operational classification.[1]

Users who require access to networks other than DSNET 1 to distribute other than SECRET information are not currently allowed access until the related security issues are resolved. The Army is investigating the use of packet encryption devices (PEDs) as an interim step to a Multi-Level Secure (MLS) encryption device to segregate the other than SECRET traffic from the rest of the network users--an approach the Air Force is currently working on. PEDs will allow users in each of the four security classification levels (U, S, TS, and SCI) to have virtually separate networks riding on one common packet network. INTERNET Protocol (IP) addressing and interoperability of devices using PEDs with the Tactical Name Server (TNS) Message Transfer Agent (MTA) must be explored.

The TPN will interface with strategic data systems (MILNET, or DSNET 1) at strategic points of presence in the Area of Responsibility (AOR) and at CONUS locations. The interface to DSNET 1 will be in accordance with the DDN security architecture. Interfaces to MILNET and DSNET 3 will be identified when the method of segregating UNCLASSIFIED traffic and TS/SCI traffic from the SECRET traffic is finalized.

The TPN will interface with other networks, such as the Air Force TASDAC system, the Marine Corps TCDN, and strategic networks (MILNET and DSNET) at strategic points of presence as required. Current plans call for each deployed Army corps, division and EAC Signal Brigade to have direct access to strategic networks. Interfaces to other tactical data networks will be accomplished where practical.

Marine Corps Data Communications Systems

The Tactical Communication Distribution Node (TCDN), currently in the prototype stage, is designed to fulfill near-term (1993-1996) joint data interoperability requirements for the Marine Corps. According to USMC combat

developers, the capabilities of the TCDN satisfy requirements of Joint Task Force components.[3] The TCDN is a candidate suite of equipment for solving the near-term joint data interoperability requirements for the Integrated Tactical-Strategic Data Network (ITSDN) initiatives under the C4I for the Warrior Concept.

As configured, the TCDN provides a host from which LANs and information systems can have access to MILNET, DSNET, ITSDN users, TPN, TASDAC and voice (potentially). For the Marine Corps, TCDN also offers a capability of interoperating directly with the Marine Corps Data Network (MCDN). MCDN is a Marine Corps wide network that connects Supporting Establishment LANs and mainframe applications. However, the TCDN has the same security limitations as the TPN. Without the use of user-provided multi-level security (MLS) devices, the TCDN can only operate at one security level. TCDN fills a near-term gap in data communications. It provides the E-Mail, file transfer and interactive terminal needs of a Marine Amphibious Group Task Force (MAGTF) or joint community.

Air Force Communications Systems

TActical Secure DAta Communications (TASDAC) is the future data communications system for the Air Force. The Air Force is currently in the procurement phase of TASDAC development. Although this system uses much of the same basic hardware as the TCDN and the same basic technology as found in the TPN, this data network is unique. The significant unique aspect of the TASDAC system is that the Air Force developers designed the use of multiple, single-level security devices into the system. In the near term, this means TASDAC can support users with information security requirements from UNCLASSIFIED through TOP SECRET with one network. It does not provide the Air Force with a Multi-Level Security (MLS) capability. TASDAC requires a significant level of effort in network management and security. It also creates unique problems when interfacing with single level secure tactical systems such as the TPN and TCDN.

Navy Data Networks

Each ship has an internal shipboard network of LANs. However, the Navy does not provide internetworking services as do the other services. The Navy uses limited bandwidth satellite and High Frequency (HF) systems to communicate with shore facilities. It uses single-channel tactical satellite, commonly called FLEETSAT, for point-to-point data transmission at low data rates. This is due in part to limited antenna size and Electo-Magnetic Interference (EMI)

considerations when placing multiple emitters aboard a small platform such as a ship. It is also due to the Navy's traditional view of independent operations when deployed.

Navy battle groups do not tend to rely on extensive communications with higher headquarters, but act based on pre-established Rules of Engagement (ROE). The Navy generally uses tactical combat net radios (High Frequency (HF), Very High Frequency (VHF) or Ultra High Frequency (UHF)) for broadcast of voice and data information within a battle group. Recently, the Navy has begun experimenting with the installation of small (4-foot) Ground Mobile Forces (GMF) satellite terminals aboard command ships in support of their Copernicus information architecture.

Endnotes

1. US Army Signa. Center and School, Tactical Packet Network (TPN) Functional Requirements Document (FRD), (US Army Signal Center, Ft. Gordon, GA, Mar 1992).

2. Captain John Weigand, USMC, HQ, USMC (CSA), DSN 224-8075, interview by the author, Ft. Gordon, GA. 7 December 1992.

BIBLIOGRAPHY

BOOKS

Allard, Kenneth C..Command, Control, and the Common Defense. New Haven, CT: Yale University Press, 1990.

Campen, Alan D..The First Information War. Fairfax, VA: AFCEA International Press, 1992.

Orr, George E. Combat Operations C3I: Fundamentals and Interactions. Maxwell Air Force Base, AL: Air University Press, 1983.

Winnefeld, James A., Johnson, Dana J..Joint Air Operations. Annapolis, MD: Naval Institute Press, 1993.

PERIODICALS

Center for Army Lessons Learned (CALL). Joint Tactical Communications. Ft.Leavenworth, KS: US Army Combined Arms Center. No. 92-1, Jan 1992.

Paige, Emmett, Jr.."Re-Engineering DoD's C3 Operations." Defense 93, n.s. 6: 15-22.

Robinson, Clarence A., Jr.."Meeting Communications Needs Champions Technical Standards." Signal 48 7 (Mar 1994): 31-33.

Skelton, Ike. "Joint and Combined Operations in the Post-Cold War Era." Military Review 9 (Sep 1993): 2-12.

GOVERNMENT PUBLICATIONS

US Air Force Deputy Chief of Staff, Command, Control, Communications and Computers. Horizon, Air Force C4I Strategy for the 21st Century. Washington, D.C.: Department of the Air Force, 1994.

US Army Signal Center, Joint Interoperability and Engineering Organization. Secure Tactical Data Network-2 Demonstration Report. Ft. Gordon, GA: Directorate of Combat Developments, 1992.

________. Secure Tactical Data Network- 3 Demonstration Report. Ft. Gordon, GA: Battle Command Battle Lab, 1993.

Chairman, Joint Chiefs of Staff. C4I for the Warrior. Washington, D.C.: US Government Printing Office, 1992.

________. National Military Strategy of the United States. Washington, D.C.: US Government Printing Office, 1993.

________. Test Pub JCS Pub 5-00.2,Joint Task Force Planning Guidance and Procedures. Washington, D.C.: The Joint Chiefs of Staff, 1988.

________. JCS Pub 6-0, Doctrine for Command, Control, Communications and Computer (C4) Systems Support to Joint Operations. Washington, D.C.: The Joint Chiefs of Staff, 1992.

Defense Communications Agency. Joint Connectivity Handbook JTC3A Handbook 8000 (Second Edition). Ft. Monmouth, NJ: JTC3A, 1989.

Defense Information Systems Agency. GCCS Common Operating Environment. Washington, D.C.: DISA, 1993

________. GCCS System Integration Plan. Washington, D.C.: DISA, 1993

Department of the Army. Army Airspace Command and Control in a Combat Zone, FM 100-103. Washington, D.C.: US Government Printing Office, 1987.

________. Army Enterprise Strategy. Washington, D.C.: Director of Information Systems, Command, Control, Communications and Computers (DISC4), 1993.

________. Army Tactical Command and Control System (ATCCS) System Management Techniques, FM 24-7. Washington, D.C.: US Government Printing Office, 1993.

________. Army Science and Technology Master Plan (Vol 1). Washington, D.C.: SARD-TL, 1994.

________. Army Science and Technology Master Plan (Vol 2). Washington, D.C.: SARD-TL, 1994.

________. Operational Terms and Symbols, FM 101-5-1. Washington, D.C.: US Government Printing Office, 1985.

________. Operations, FM 100-5. Washington, D.C.: US Government Printing Office, 1993.

Department of Defense. Final Report to Congress: Conduct of the Persian Gulf War. Washington, D.C.: US Government Printing Office, 1992.

Joint Interoperability and Engineering Organization. Secure Tactical Data Network-4 Demonstration Report. Ft. Huachuca, AZ: JITC, 1993.

Naval Command, Control, and Ocean Surveillance Center. User Interface Specifications for Navy Command and Control Systems version 1.2. Washington, D.C.: ONI-25, 1992.

Space and Naval Warfare Systems Command. Operations Support System (OSS) Executive Overview. Washington, D.C.: SPARWARSYSCOM, 1992.

USACECOM. Organizational and Operational Plan (O&OP) for the Family of Maneuver Control System (MCS). Ft. Leavenworth, KS: US Army Combined Arms Center, 1989.

ORIGINAL MANUSCRIPTS

Deyer, Hervert D..Joint Tactical Command, Control and Communications (C3) Interoperability. Carlisle Barracks, PE: U.S. Army War College, 1990.

Martin, W.R.. C3 Interoperability Issues: An Overview of GOSSIP Network Conformance Testing in the Evolution of the Defense Information System Network (DISN). Monterey, CA: Naval Postgraduate School, 1992.

McKiernan, D.D.. Command, Control and Communications at the VII Corps Tactical Command Pcst: Operation Desert Shield/Desert Storm. Carlisle Barracks, PA: Army War College, 1992.

Walker, R.P., Corlis, G.A., Cheatham, E.C., Schelber, L.B.. Assessment of Potential for Commonality of ADP for Army and Marine Corps C2 in selected Functional Areas (Volume 1). Alexandria, VA: Institute for Defense Analysis, 1989.

________. Assessment of Potential for Commonality of ADP for Army and Marine Corps C2 in selected Functional Areas (Volume 2). Alexandria, VA: Institute for Defense Analysis, 1989.

BRIEFINGS

Air Combat Command (ACC). Contingency TACS Automated Planning System. Presented at Ft. Leavenworth, KS, 1-2 Mar 1993.

Air Combat Command (ACC). CTAPS Migration Strategy. Presented at Ft. Leavenworth, KS, 1-2 Mar 1993.

SAIC Corp. GCCS Roadmap and Demonstration. Presented to LTG Edmonds (JCS J-6) at Washington, D.C., 7 Sep 1993.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
U.S. Army Command and General Staff College
Fort Leavenworth, KS 66027-6900

2. Defense Technical Information Center
Cameron Station
Alexandria, VA 22314

3. LTC Herbert F. Merrick, Jr.
Department of Joint and Combined Operations
USACGSC
Fort Leavenworth, KS 66027-6900

4. CH (MAJ) Edward K. Maney
Department of Joint and Combined Operations
USACGSC
Fort Leavenworth, KS 66027-6900

5. COL Kenneth R. Garren
Roanoke College
221 College Lane
Salem, VA 24153-3794

6. COL Tom Nicholson
Battle Command Battle Lab
ATTN: ATZH-BL
Ft. Gordon, GA 30905

7. COL Robert Forrester
Director of Combat Developments
ATTN: ATZH-CD
Ft. Gordon, GA 30905-5000

8. LTC Kenneth Bostelman
DA DISC4
ATTN: SAIS-C4T
Washington, D.C. 20310-0107

9. LTC William Clingempeel
Hq, 13th Sig Bn
ATTN: AFVA-13SI-CDR
Ft. Hood, TX 76545

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 4 / 5 / 94

2. Thesis Author: Major James P. Kohlmann

3. Thesis Title: Winning the Information War: Challenges of providing interoperable information system support to an Army-led Joint Task Force.

4. Thesis Committee Members Signatures:

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

A B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

S--------SAMPLE-------------SAMPLE-----------------SAMPLE-----------S

Limitation Justification Statement	Chapter/Section	Page(s)
Direct Military Support (10)	Chapter 3	12
Critical Technology (3)	Sect. 4	31
Administrative Operational Use (7)	Chapter 2	13-32

---------SAMPLE-------------SAMPLE-----------------SAMPLE------------

Fill in limitation justification for your thesis below:

Limitation Justification Statement	Chapter/Section	Page(s)

7. MMAS Thesis Author's Signature: ____________________

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).